PATENT ABSTRACTS OF JAPAN

(11)Publication number : **08-096043**

(43)Date of publication of application : **12.04.1996**

(51)Int.Cl. G06F 17/60

G06F 19/00

H04Q 7/38

(21)Application number : **07-264673**

(22)Date of filing : **20.09.1995**

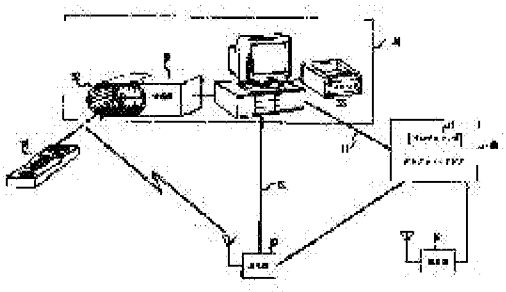
(71)Applicant : **AT & T CORP**

(72)Inventor : **PARTRIDGE III B WARING**

(30)Priority

Priority number : **94 310441** Priority date : **22.09.1994** Priority country : **US**

(54) METHOD FOR ASSURING ACTION AND ARRANGEMENT FOR PROVIDING CREDIT



(57)Abstract:

PROBLEM TO BE SOLVED: To provide arrangement for providing e.g. credit to a customer via cellular system telephone set with an authorized transaction controller.

SOLUTION: The arrangement is provided e.g. by starting up the cellular system telephone set 10 by the customer requesting the credit in purchasing commodities or services from traders, authorizing the cellular system telephone set 10 to the base stations 20, 50 of the service provider of the cellular system telephone, and setting up coupling so as to obtain the credit. The customer obtains the credit by transmitting the peculiar sequence different from the ordinary number sequence corresponding to a callee telephone number. The identification code of the trader and the desired amount of credit are included in the sequence.

LEGAL STATUS

[Date of request for examination] 10.03.1998

[Date of sending the examiner's decision of rejection] 18.06.2002

[Kind of final disposal of application other than the examiner's decision of rejection or application converted registration]

[Date of final disposal for application]

[Patent number]

[Date of registration]

[Number of appeal against examiner's decision of rejection]

[Date of requesting appeal against examiner's decision of rejection]

[Date of extinction of right]

CLAIMS

[Claim(s)]
[Claim 1] (A) the starting step which starts the radio communication equipment (10) formed in the communication link, and (B) -- the authentication step which attests discernment of this radio communication equipment based on the signal which this radio communication equipment sends, and (C) -- the action guarantee approach of guaranteeing action for the user characterized by having the action execute step which performs specific action permitted by this radio communication equipment.
[Claim 2] The authentication step (aforementioned [B]) is an approach according to claim 1 characterized by using the protocol which is selectively equivalent to a part of registration protocol [at least] which said radio communication equipment uses when using said radio communication equipment for communication link utilization at least.
[Claim 3] The authentication step (aforementioned [B]) is an approach according to claim 1 characterized by using the protocol which is selectively equivalent to the registration protocol which said radio communication equipment uses when using said radio communication equipment for communication link utilization at least.
[Claim 4] Said action for said user is an approach according to claim 1 characterized by being the credit supply step which supplies said user with a credit.
[Claim 5] Said credit supply step is an approach according to claim 4 characterized by being carried out by the communication service provider who provides said radio communication

equipment with communication service.
[Claim 6] Said credit supply step is an approach according to claim 4 characterized by being carried out by communication service non-providers other than the communication service provider who provides said radio communication equipment with communication service.
[Claim 7] Said action for said user is an approach according to claim 1 characterized by being the guarantee control signal transmitting step which transmits a guarantee control signal to a specific destination.
[Claim 8] Said action for said user is an approach according to claim 1 characterized by being the control signal transmitting step which transmits a control signal to a destination.
[Claim 9] Said destination is an approach according to claim 8 characterized by being a home controller base station (50).
[Claim 10] Said destination is an approach to a publication in claim 8 characterized by being the home controller base station (60) which converses with the signal provider who offers a signal to a television set.
[Claim 11] Said credit supply step is an approach according to claim 4 characterized by having the step which transmits the string data containing transaction password partial sequence, a credit golden frame part train, ID partial sequence, and verification partial sequence to a credit offer center.
[Claim 12] In the credit offer arrangement which provides the 1st party who has with a credit with a credit offer center (40) and relation with radiotelephony for the profit of the 2nd party (A) 1st means to identify said radiotelephony to said credit center using the discernment protocol which said radiotelephony uses for radiocommunication, and the suiting discernment protocol, (B) The 2nd means which connects discernment of said 2nd party and the credit total amount of money with the radiotelephony identified by said 1st means, (C) Credit offer arrangement said whose credit center is characterized by having 3rd means to communicate the acknowledgement status to said 2nd party.
[Claim 13] The basic factor of said 1st means, said 2nd means, and said 3rd means is arrangement according to claim 12 characterized by being under control of said credit offer center.
[Claim 14] Said 1st means is arrangement according to claim 12 characterized by having a communication link between a cellular phone base station, this cellular phone base station, and said credit center.
[Claim 15] Said 1st means is arrangement according to claim 12 characterized by having a sending set (30) within the premises of said 2nd party in order to communicate with said credit center.
[Claim 16] Said sending set of the premises of said 2nd party is arrangement according to claim 15 characterized by communicating with said credit center through a cellular phone base station.
[Claim 17] The basic factor of said 1st means, said 2nd means, and said 3rd means is arrangement characterized by arranging within the premises of said 2nd party.
[Claim 18] Said 1st means is arrangement according to claim 17 characterized by having a receiving set (31) in order to communicate with said radiotelephony further.
[Claim 19] Furthermore, arrangement according to claim 18 characterized by having a means to distinguish the transmission from said radiotelephony from the transmission from other radiotelephony.

DETAILED DESCRIPTION

[Detailed Description of the Invention]
[0001]
[Field of the Invention] This invention relates to radiotelephony and relates to the utilization process of the radiotelephony which guarantees action for the holder of this radiotelephony especially.
[0002]
[Description of the Prior Art] Current radiotelephony is chiefly used for the communication link. On the other hand, in order to guarantee action for a user, another equipment like the example of a degree is used. For example, TV, VCR, etc. are controlled using remote control of an infrared method. Moreover, it guarantees entering into a house using the key of a house. Moreover, it is the example which obtains a customer credit using a credit card. It is because control is performed by this user and the result of a certain request or a profit is got, because all of these activities can be classified with a "control transaction."
[0003] Time of giving the example which it is the no charge which is in these transactions, for example, guarantees going into its own house, the example which controls reception of the free channel of TV can be performed. Moreover, the example which a certain transaction is a charge, for example, guarantees going into a theater, the example which chooses the "pay" TV channel per viewing and listening, the example which obtains a customer credit can be given. The object of this invention is offering the system which solves the technical problem about the following control transaction, and is as follows.
[0004]
[Problem(s) to be Solved by the Invention] In the case of the control transaction of the system and charge to which a user is made to use that radiotelephony for and a control transaction is made to perform, a system distribution with which the credit account in which the holder of this radiotelephony has the cost of this control transaction to that radiotelephony service provider or another party is burdened is desired.
[0005]
[Means for Solving the Problem] This invention forms the transaction controller which guaranteed action for a user using radiotelephony and was guaranteed by it. This procedure's starting of this radiotelephony bases it on the Challenge Handshake Authentication Protocol concerning it. Once this radiotelephony is attested, ****** with which the credit account in which control command is emitted by that radiotelephony (or that radiotelephony effectively), and the holder of this radiotelephony has the credit total amount of money to this radiotelephony service provider if needed is burdened will be permitted, and it will consider as liability at it.
[0006] In order to purchase it in the utilization which asks for acceptance of a customer credit (for example, goods and the vendor (it only abbreviates to a contractor below) of service), the customer who asks for a credit carries out as follows. This customer starts that radiotelephony, attests this radiotelephony to this radiotelephony service provider through that local base station, and he progresses so that a "dialogue" may be established, in order to get a credit. A credit transmits the characteristic sequence which can be made into a different sequence from a number sequence corresponding to a characteristic sequence, i.e., the called party telephone number, to a radiotelephony service provider, and is usually obtained. Although there is a contractor ID code (what identifies that vendor) and it is still more natural, a request credit amount of money is one of those which are included in this sequence, and other information, for example, information, such as a purchase item and service to receive, can be mentioned to them further again.

[0007] With another gestalt of operation of this invention, the information transmitted to that base station is monitored, the information about the request credit amount of money is added with this contractor, and this contractor's wireless receiving set has and passes [organize and] through the account of that credit offer organization, i.e., this radiotelephony holder, and transmits this information. The communication link with this credit offer organization can be performed through radiocommunication or a wire communication. If it is judged that the demand to this credit is appropriate, a message will be transmitted to this contractor, the supply of a credit will be permitted, and this transaction will be ended successfully. If the random signal of a radiotelephony base station can be combined, the signal which can be attested can be transmitted and it is attested when it is the utilization whose control transaction of this does not need to access that radiotelephony holder's credit line, and when only authentication is important (for example, when unlocking that home garage door using radiotelephony), that control transaction will be performed.
[0008]
[Embodiment of the Invention] The gestalt of operation of this invention is illustrated in the following order, and is explained. It starts from the supply of the customer credit with which authentication and amount-of-money exchange become very important first, and explanation of the process of acquisition. Next, the process to which authentication accesses an indispensable home is explained. The process by which only the function of a command and control controls an important device like TV, for example is explained to the last. The following explanation is given by taking up the protocol used for a cellular phone and a cellular phone. However, when this invention is contrasted with other radiotelephony, it is still larger than the case of utilization of a cellular phone, for example. [of his understanding here]
[0009] 1. In a credit supply current, the process which supplies a customer credit is the considerably common actuation. For example, an organization like a bank provides a customer with a credit, this customer is supplied with a credit card, and this customer purchases goods and a screw using this credit card. If goods and service are purchased, it will be charged to this customer's card, this organization will send a description to this customer at the deadline for an invoicing cycle, and this customer will offset the credit with which it supplied that organization by the end of the payment date. Although it is natural, those who ask for acquisition of a credit card need to find the organization which supplies this credit. By the way, although it is not an especially difficult failure for many people to find the organization which supplies a credit, the following point attracts attention.
[0010] It attracts attention that it has much those who already have two or more communication link business objects (local exchange service, long-distance communication link business object, cel communication link business object) and loan relation as for the customer of a credit. The problem which cannot use this diffused relation for supplying a general customer credit here, or asks that propriety arises. Since people who are carrying the cellular phone are becoming a large number, if this relation is used and it can process together with a credit card, to be sure, it is convenient. Arrangement and the process of explaining below offer this function. Although a cellular phone 10 is shown in drawing 1 , this is used in order to radiocommunicate with a base station 20. A base station 20 communicates with the credit center 40, and the credit center 40 communicates with a contractor's device 30. Moreover, a base station 50 also communicates with the credit center 40.
[0011] Although the cellular call-service provider who operates the credit center 40 and base stations 20 and 50 may belong to the same organization, it is not necessary to restrict to it. It is

usual that the credit center 40 is a billing handling category in the organization which provides that user with this cellular call service. For example, the following case is assumed. A base station 20 belongs to the cellular call-service provider A, and a base station 50 belongs to the cellular call-service provider B, and the right holder of a cellular phone 10 has privity of contract with the cellular call-service provider B. Furthermore, the credit center 40 is made into the cellular call-service provider's B billing handling device. Moreover, a channel 21 is a channel which combines a device 30 with the credit center 40, and is the channel of a cable or wireless.
[0012] If authentication of an insurance guarantee can be acquired, since it is the communication link between a device 30 and the credit center 40, an either usual protocol can be used. The fundamental transaction about the case where a customer credit is acquired charges the amount of money chosen as the cellular phone 10 in the credit center 40 at the account of pair Perilla frutescens (L.) Britton var. crispa (Thunb.) Decne., and a contractor notifies this contractor of having obtained the benefit from this accounting to this radiotelephony holder's account. however, this comes out in the premise that a cellular phone 10 is in a right customer's hand. Since it is simple, when a query is in the justification of the possessor of this cellular phone, the protocol which requires it is not described here. The case of utilization, such as a customer's personal identification code and voice authentication, can be mentioned to this.
[0013] However, it may be said that recognizing here offers the guarantee whose both of that customer and contractor receive the profit of this supply credit in one in these technical problems. Another technical problem is offering this interaction by the approach by which insurance's was guaranteed that neither this customer nor its contractor gets disadvantageous profit. Still more nearly another technical problem is offering this interaction so that a third party's may not get disadvantageous profit by this communication link and a profit's may be obtained again. Although these objects show the example of the following patent made into an illustration here to drawing 2 here where it considers as reference, they are realized by the protocol. it -- United States patent No. 5,204,902 and Reeds ** -- refer to issuance on April 20, 1993. This Reeds's and others patent is described briefly. Here, there are the following in each cellular phone.
[0014] That is, there is digital string data of "common restricted data" (SSD), this is drawn from association of hash processing of a secret key (A-KEY), and there is that cellular phone device number (ESN) further, and there is that cellular phone allocation number (MIN1), random string data is one of those which each cellular phone has further, and the organization where this cellular telephone user has business relation chooses this as them. As an example of representation, this organization has the privity of contract which pays accounting which it is a cellular call-service provider, and this cellular call-service provider and this customer "signed", that is, was produced. A cellular call-service provider is usually limited to the geographical area of specification [the area].
[0015] This area is that customer's "home" cellular call-service geographical area (home CGSA). The home CGSA of a cellular phone 10 presupposes that it is a base station 50 on account of explanation. The base station 20 of a cel where a cellular phone 10 exists presupposes that he is the "visiting place" host CGSA. This SSD train is divided into the SSDA train of two trains, and a SSDB train. This SSDA train is used for authentication and a SSDB train is used for communication link codes. Next, actuation explains. Each cel of a cel communication network is served by base station like (base stations 20 and 50). this base station -- being certain -- it chose -- although broadcast of the random sequence (RAND) is repeatedly carried out at a rate -- a security enhancement sake -- comparatively -- frequency -- many (for example, duration time of

a cel call of most more frequently) this RAND is changed.
[0016] If a power source is put into the cellular phone which is in a certain cel, this RAND sequence is received, and that cel will be told about itself and will be answered (a cellular phone 10 receives RAND which a base station 20 transmits). This is a registration process and is shown by the lines (process) 11, 12, and 13 of drawing 2 . Processes 11, 12, and 13 are explained still more concretely. This cellular phone connects that ESN train and MIN1 train with that SSDA train and RAND train, carries out hash processing of the obtained string data, and acquires that AUTHR train. Next, this cellular phone transmits that AUTHR train to that base station with a RAND train, an ESN train, and MIN1 train for a check.
[0017] Although it swerves from explanation here, the reason for transmitting this RAND signal is that that base station has changed that RAND between the times of the time of a cellular phone 10 receiving RAND and its base station receiving AUTHR, this is an option, because it is because that base station can memorize the RAND train of that last easily. This base station opts for the discernment which detects this ESN train and MIN1 train and by which that cellular phone was asserted from here, and discernment of that home CGSA. Although it swerves, in order to identify this home CGSA, explanation needs to apply an algorithm to this ESN train and MIN1 train, or needs to refer for it to a database.
[0018] Although a base station 20 is this home CGSA and this is a base station 50 in the example of drawing 1 , hash processing of the string data which will receive this SSD train from now on, and might be combined with that RAND train and ESN train, and MIN1 train in this SSDA train is carried out, and the AUTHR train of that version is acquired. Next, this base station compares the AUTHR train of that version with the AUTHR train of that receiving version. Coincidence of these two string data determines the cellular phone as a right thing. In order that it may be transmitted to that cellular phone from this base station and "O.K." signal (line 13) may communicate further to this, the information about the specific frequency which this cellular phone needs to use is included.
[0019] If registered by this handling base station, although this cellular phone can start a call, this will be performed in the process which connects with other string data that call-ed telephone number that exists at least. Namely, as for this cellular phone, a new AUTHR train can also transmit further MIN3 train which is the information on that called party with that RAND train and ESN train, and MIN1 train. This new AUTHR train is acquired from RAND, ESN, MIN1 and MIN3, and hash processing of connection of SSDA (it is because there is no call which does not illustrate to drawing 2 , because is made into a third party). Once a dialogue with this base station is set up, if a actual information communication link is a request, it can progress by being enciphered by SSDB.
[0020] In order to hold security furthermore, although this base station can require a reconfirmation certificate at any time, this is performed like said initial registration. Next, it returns to the technical problem which obtains a customer credit to the holder of the cel telephone 10. it is the need, in order to supply a credit and to charge this user's account in the credit center 40 -- the following step is most contained in a fundamental protocol.
(A) They are the required information about that account that communicates with the credit center 40 and charges it, the step which offers the total amount of money which charges that account, and the step which notifies returning that demand total amount of money to this contractor, and considering as a claim by the (B) contractor's device 30. It is convenient, if a step can furthermore be added, for example, the following term can be guaranteed.
[0021] It can mention guaranteeing not adding [which guarantees that return / which guarantees

charging that offer credit to a right account / that demand total amount of money to a right contractor further, and it considers as a claim] the present or future damage to the credit center 40 or the user of a cellular phone 10 by the trespasser further again at this contractor etc. A detail protocol with the following step is shown as an example of the simple form.
(A) Although this contractor offers a code peculiar to that customer, this is a characteristic code which identifies this contractor in the credit center 40 (line 18 of drawing 2).
[0022] (B) This customer adds a matter like the example of a degree to a cellular phone 10. For example, it is a prefix as shown in "an asterisk and 9", is that contractor's ID code further, and is the total amount of money which needs to charge this customer's account further, needs to return to that contractor, and needs to be made into a claim. This forms MIN2 train.
(C) A cellular phone 10 is registered previously in a base station 20, and the data of a step (B) are inputted into that buffer, a that "transmitting" command is answered, and that MIN2 train, a RAND train, an ESN train, MIN1 train, and an AUTHR train are transmitted, however this AUTHR train is acquired from RAND, ESN, MIN1 and MIN2, and hash processing of connection of SSDA (line 14 of drawing 2).
[0023] (D) A base station's reception of this transmit information admits being what this is not usually a call (from for example, that "asterisk and 9" train), and is going to arrive at the credit center 40. It is answered, the credit center 40 is contacted and the related information is told. That is, this is the ESN and data of MIN1 and MIN2 (line 17 of drawing 2). It guarantees effectively that the Challenge Handshake Authentication Protocol of a base station 20 is a telephone corresponding to [in fact] the ESN and MIN1 which received in a cellular phone 10, therefore the credit center 40 is located in the location which deserves that the customer of MIN1 gets a credit, or asks for the right or wrong.
[0024] (E) If the credit center 40 determines that it needs to supply radiotelephony 10 with a credit, further probably as for this credit center, an acknowledgement code will be transmitted to a contractor's device 30 also like that cellular phone (lines 15 and 16 of drawing 2). The transaction of this request is successfully ended by reception of this acknowledgement. Actual copy **** of this credit to this customer's credit account is performed like usual, and this can change the tariff charge rate to a cellular phone 10, and can also perform it so that it may be carried out with "900 Service."
[0025] It is that this contractor needs to provide this customer with that code with the protocol of disclosure above in a point somewhat troublesome [one], and it is expected that an error arises if this step is performed by voice communication. It is because the process which a little thing for which the credit center 40 needs to contact a contractor's device is inconvenience, because this needs utilization of the database which translates this contractor's code into the telephone number (usually), and sets up a communication path takes time amount further further again. However, these faults are conquered in the modification to which slight deformation, for example, this contractor, is rather another path, and he contacts the credit center 40, and the modification in which this contractor transmits that identification code to that credit center electronically.
[0026] Although it is natural, it is necessary to link the communication link between the radiotelephony 10 through a base station 20, and the credit center 40 with the communication link between a contractor 30 and the credit center 40 (for the purpose of being related). This link can be set up by that contractor that has agreed on the activity of the selected transaction password (TP train), and this customer. It seems that this string data shall be random, and shall be transitional, for example, shall merely be used only at once. This TP train can be inputted instead of this customer being that contractor's ID code, it can be transmitted to a base station 20,

and that contractor can use the same TP for a communication link of a contractor with the credit center 40.
[0027] This TP train can be communicated from that contractor with voice to this customer, and this customer can insert this code in that cel telephone. Risk of a neighboring cellular phone joining this communication link accidentally, undertaking that credit amount of money, and considering as liability by this, is abolished. Since this TP train is merely used only at once, a trespasser does not have that value, and it is that an error at this step only makes that transaction go wrong clearly. When this arises, this customer and its contractor can reinput and retry this TP train (or a different TP train). Also when based on this deformation protocol, although that telephone communication is a front passage, it has the next point of difference here.
[0028] It contacts that credit center, clarifies an identity, and offers this TP train, and, in a suitable case, this contractor's device receives acknowledgement or authorization from that credit center. In order that the credit center 40 may help to link TP train which this contractor offered to the communication link by radiotelephony 10, it is convenient that a contractor's device 30 contains ESN and MIN1 of radiotelephony 10. This protocol is shown in drawing 3 . Although it is natural, a device 30 needs to receive the information on ESN and MIN1 from radiotelephony 10, and this can realize it with the receiver 31 which accompanies a device 30. It is possible that the customer who can use this receiver as a low sensibility receiver, because purchases that goods and service is in the neighborhood of this receiver, and this contractor wishes not to receive the transmission from an adjoining cellular phone again.
[0029] Reception of only a right cellular phone can be guaranteed by the approach except using a low sensibility receiver. For example, it can set so that all reception from a cellular phone that does not transmit this TP train for the receiver of a device 30 may be rejected. Or although a device 30 can have the metal shroud 32 around an antenna 31, however inserts the antenna of radiotelephony 10 here, an antenna 31 receives only the signal by this. If a receiver 31 is introduced into a device 30, however the communication link between the unrelated telephone 10 and a base station 20 may not surely carry out or there may be, it is not necessary to carry out directly. That is, a device 30 catches transmission of radiotelephony 10, whatever the data for which it asks, adds it, and does = (using pass 22 of drawing 1) transmission of this joint information through a base station 20 to the credit center 40.
[0030] Or a device 30 can bypass a base station 20, can transmit the data to the credit center 40 directly, and a preprocessor 42 receives the data and it emulates the registration process of a base station 20 here. As shown in drawing 4 , a contractor's device 30 acquires the RAND train from a preprocessor 42, and transmits it to radiotelephony 10. This contractor can transmit that TP train to the user of radiotelephony 10 simultaneously. Radiotelephony 10 generates the following string data. There are that transaction password train (TP), an ESN train, and MIN1 train, and although it is an option, there is MIN2 train in this, and there is an AUTHR verification train (that TP train is embedded in this AUTHR train) in it further.
[0031] Next, a device 30 transmits this information to a preprocessor 42, and, probably adds that RAND train to this TP train, its total amount of money, its ID code, and a pan. Although a preprocessor 42 checks the justification of the user who demands a credit, it analyzes this AUTHR train to other data which the device 30 transmitted, and it performs it, supplies a credit, or determines that right or wrong. next, this decision -- a device -- 30 HE, although it is an option further, it is transmitted to radiotelephony 10. It can carry out by the ability of this contractor providing that customer with print-out, and this customer can sign this print-out according to a request, and a check with the document of the amount of money which charges this customer's

account can be considered as backup verification of this accounting. By drawing 1 , equipment 33 shows this printer.
[0032] The device is completely the usual device [hardware / required for the system shown in drawing 1]. For example, a cellular phone 10 is also the usual cellular phone, and base stations 20 and 50 are the usual base stations similarly. As for this contractor's device, it being necessary to carry out by being a still easier receiver, or it is resemblance at the receiver of a base station 20 is only only distinguishing an input signal so that priority's may merely be given to a right input signal by reception of a signal. In this case, it is expected that the cellular phone of the customer who asks for purchase will 2-double-approach at least compared with the following cellular phone which approached most to that contractor's receiver. A shroud 32 is an effective thing which makes an error small at such distinction.
[0033] Then, the distinction based on the power to input is easy, and effective. However, such [again] distinction can remember that it can carry out only by checking that the TP train is included in the communication link from a cellular phone 10. It is necessary to embed from this at AUTHR and, and that cellular phone needs to output this TP train to "the free space which is not although interrupted." A means to add information to a contractor's device 30 at those received data in addition to this receiver, and to transmit this data to the credit center 40 is required. Such a device is the usual PC, or it can correct by specific hardware arrangement, and is low also in respect of a price also in respect of various functions, and can be realized now easily.
[0034] It can use by any class of printer ordinarily used for the printer about the usual credit card here now. About the credit center 40, this is office which serves as a communication link and a main role of a database in almost all cases, and does not differ from a current cellular phone provider's business office so.
[0035] 2. -- the home feedback above -- after shopping like the example which goes out privately, the holder of a cellular phone asks for access to the home, and asks for unlocking of a garage door under control of the same cellular phone. Here, it is not necessary to apply the credit center 40 for this object because, and a credit is not supplied (in accounting which it corrects, for example, this control transaction is performed by that base station, and is undertaken to that contribution, naturally, it excepts). The task which described the outline above is only the example of control of one garage door unlocking machine, and although it is not a requirement, it also has the example in which a communication link is included further as follows. In the example of a gestalt of communicative implementation, as for a garage door unlocking machine, a decode means is added with a cellular phone receiver.
[0036] Next, actuation explains. This garage door unlocking machine can be registered in that cellular phone base station, and this base station can incorporate that SSDA train and SSDB train there. Although this base station communicates with that garage door unlocking machine by the guaranteed method and this of the main point is almost the same as that of the case of other cellular phones, a point of difference is only the one direction communication link to a garage door receiver from this base station. If this cellular phone 10 wants to make that garage door unlocked, when wanting, it is required that it should be made to call to this garage door receiver in that base station, and series-of-commands data should be transmitted to that receiver. The following are one of those which are included in this data stream.
[0037] there is a random number (RANDX) in it -- having -- the holder of this cellular phone -- " -- it is devoted -- having -- " -- hash processing of this random number is carried out by the key (B-KEY) (are that TP train and a transaction password and was accumulated to this transaction)

further in the cel telephone 10 in **. As mentioned above, there is a decode means in this receiver and this is a decode means to collect the string data which carried out hash processing by that B-KEY. When this decode random number is equivalent to the random number received in "the free space which is not although interrupted", that garage door is unlocked. This protocol is shown in drawing 5 , and lines 11, 12, and 13 show that registration process here, as drawing 2 was described.

[0038] It turns out that the protocol with which these cellular phones differ for a while by drawing 5 from the protocol of the usual telephone association is followed here. That RANDX train and B-KEY (RANDX) train are promptly added instead of waiting for the display to which this called party telephone number (MIN3) was only transmitted and which this called party specifically answered from that base station. This is easily performed by choosing this with this cellular phone, although the RANDX train which a user supplies to the sequences which this cellular phone can recognize easily (it reaches, otherwise does not correspond to effective string data), "8", and rightness continues. [for example,] Or although a cellular phone 10 is thinking, this MIN3 signal is transmitted and the remainder of that sequence is transmitted for a clear two SENDO signal to waiting and a degree.

[0039] In the example of a gestalt of the operation which does not include a communication link, this cellular phone base station operates with the still more nearly following semantics. That is, shortly after this cellular phone has a dialog with that base station automatically and turns on this cellular phone, notice is submitted itself and it is registered. For better or worse, if it puts in another way, if this cellular phone is turned on, notice will be itself submitted to that base station, and it will register with it. This activity does not usually generate accounting to that cellular phone holder's credit account. It is this object to unlock this garage door without the help from that base station in the example of a gestalt of the operation which does not include a communication link beyond this registering point.

[0040] Although this is attained by many approaches, the following point is surely required for it. The signal transmitted to this base station where it follows "O.K." signal of a line (drawing 5) 13 needs to be what is not understood in this base station. On the contrary, this garage door receiver needs to be aligned with that transmission from that cellular phone, and that transmission needs to understand it. This can be attained like the example of a degree. For example, although this garage door receiver is "O.K." signal of that base station, however the signal directed that this operates on a specific frequency to this cellular phone, this transmission is monitored and it can realize. Next, this receiver can be itself aligned with that same frequency, and can catch transmission of this cellular phone.

[0041] If a cellular phone 10 transmits the signal of the line 25 of drawing 5 next as shown in drawing 6 , this receiver will monitor it, it will be decoded and that garage door will answer there. or [MIN3 being string data which the base station does not recognize, or deleting AUTHR in such an example of a gestalt of operation,] -- or it only changes and refusal is made to cause by the base station Or if the "8" sequence is inserted in a cellular phone 10, it can align with the fixed appeal frequency used for registration itself. This garage door unlocking machine can be aligned with such implementation fixed in that appeal frequency. Said example of garage door unlocking is an example, and can mention other control utilization, for example, unlocking of an automobile door or a house, and an activating alarm, and these are also included by the technical range of this invention here.

[0042] 3. If it can access to the home of control ****** as a request, the holder of a cellular phone 10 can ask for control of various devices. It is not that security has an interest like [in said

utilization of two examples] in such utilization. It is desirable not to include this base station in such control utilization from a viewpoint of a public policy further again. In the case of the latter, it can carry out only by changing the clock frequency of this cellular phone into the band which is not covered by this base station. Next, actuation explains. It operates on the frequency as which the home controller base station of itself is located at each home, and this was chosen. In a switch or code "driven in", this cellular phone can be made into "home controller" mode, and this cellular phone has a dialog only with that home controller base station in this mode.
[0043] next, what kind of control can perform it also for allocation **** to it using the approach usual in this home controller base station. Although this authentication process can be performed as mentioned above, it is carried out to the bottom of control of this home controller base station. That is, this home controller base station can include the function which attests that cellular phone as a home controller based on the interaction of that request, does not need to restrict it to it, or can also carry out it selectively. For example, it is also possible to be able to change TV channel as a home controller using this cellular phone, therefore to ask for a certain security processing probably.
[0044] However, although it can also have a dialog that television signal supply origin again using this cellular phone, it is not necessary to ask for security here. Purchasing by such interaction is also possible, and even if the owner of a home controller makes a visitor use this home controller base station as a conduit tube and it does not care about it, it does not interfere. Arrangement of disclosure is shown in drawing 7 above, the home base station 60 is here, there are further various home controllers 61, this controls a device, there are television "set top box" 62, and there is television 63, and there is a means 64 by which it can have a dialog the goods [which were further advertised on this television] and/or supply origin of service in this device.
[0045] Although it is also possible to make such a means into a part of the set top books and this returns a signal to the supply origin (it illustrates) of the television signal, it is not necessary to restrict to it. What should be written in addition here does not restrict the above explanation of this invention to a cellular phone. Although the function of disclosure is above realizable with any wireless means of a class, it may be the utilization it is the case where such a means has suitable authentication capacity to utilization at hand, however a desired authentication function is not important or is completely above unnecessary like explanation. Although the various modifications of this invention can consider the above explanation about the example of 1 gestalt of operation of this invention if it is this contractor of this technical field, each of they is included by the technical range of this invention. In addition, the reference number indicated to the claim is for an understanding with easy invention, and should not be interpreted as restricting the technical range.
[0046]
[Effect of the Invention] As stated above, it is the transaction controller attested by this invention, a customer credit can perform amount-of-money exchange using a cellular phone, and a home garage door can be made to be able to unlock, it can use for the goods of a television advertisement, or the dialogue of service further, and the attested effective transaction controller can be offered, and the useful radiotelephone system of the intensive use which added multifunctional utilization to communication link utilization further can be offered.

TECHNICAL FIELD

[Field of the Invention] This invention relates to radiotelephony and relates to the utilization process of the radiotelephony which guarantees action for the holder of this radiotelephony especially.

PRIOR ART

[Description of the Prior Art] Current radiotelephony is chiefly used for the communication link. On the other hand, in order to guarantee action for a user, another equipment like the example of a degree is used. For example, TV, VCR, etc. are controlled using remote control of an infrared method. Moreover, it guarantees entering into a house using the key of a house. Moreover, it is the example which obtains a customer credit using a credit card. It is because control is performed by this user and the result of a certain request or a profit is got, because all of these activities can be classified with a "control transaction."
[0003] Time of giving the example which it is the no charge which is in these transactions, for example, guarantees going into its own house, the example which controls reception of the free channel of TV can be performed. Moreover, the example which a certain transaction is a charge, for example, guarantees going into a theater, the example which chooses the "pay" TV channel per viewing and listening, the example which obtains a customer credit can be given. The object of this invention is offering the system which solves the technical problem about the following control transaction, and is as follows.

EFFECT OF THE INVENTION

[Effect of the Invention] As stated above, it is the transaction controller attested by this invention, a customer credit can perform amount-of-money exchange using a cellular phone, and a home garage door can be made to be able to unlock, it can use for the goods of a television advertisement, or the dialogue of service further, and the attested effective transaction controller can be offered, and the useful radiotelephone system of the intensive use which added multifunctional utilization to communication link utilization further can be offered.

TECHNICAL PROBLEM

[Problem(s) to be Solved by the Invention] In the case of the control transaction of the system and charge to which a user is made to use that radiotelephony for and a control transaction is made to perform, a system distribution with which the credit account in which the holder of this radiotelephony has the cost of this control transaction to that radiotelephony service provider or another party is burdened is desired.

MEANS

[Means for Solving the Problem] This invention forms the transaction controller which guaranteed action for a user using radiotelephony and was guaranteed by it. This procedure's starting of this radiotelephony bases it on the Challenge Handshake Authentication Protocol concerning it. Once this radiotelephony is attested, ****** with which the credit account in which control command is emitted by that radiotelephony (or that radiotelephony effectively), and the holder of this radiotelephony has the credit total amount of money to this radiotelephony

service provider if needed is burdened will be permitted, and it will consider as liability at it.
[0006] In order to purchase it in the utilization which asks for acceptance of a customer credit (for example, goods and the vendor (it only abbreviates to a contractor below) of service), the customer who asks for a credit carries out as follows. This customer starts that radiotelephony, attests this radiotelephony to this radiotelephony service provider through that local base station, and he progresses so that a "dialogue" may be established, in order to get a credit. A credit transmits the characteristic sequence which can be made into a different sequence from a number sequence corresponding to a characteristic sequence, i.e., the called party telephone number, to a radiotelephony service provider, and is usually obtained. Although there is a contractor ID code (what identifies that vendor) and it is still more natural, a request credit amount of money is one of those which are included in this sequence, and other information, for example, information, such as a purchase item and service to receive, can be mentioned to them further again.
[0007] With another gestalt of operation of this invention, the information transmitted to that base station is monitored, the information about the request credit amount of money is added with this contractor, and this contractor's wireless receiving set has and passes [organize and] through the account of that credit offer organization, i.e., this radiotelephony holder, and transmits this information. The communication link with this credit offer organization can be performed through radiocommunication or a wire communication. If it is judged that the demand to this credit is appropriate, a message will be transmitted to this contractor, the supply of a credit will be permitted, and this transaction will be ended successfully. If the random signal of a radiotelephony base station can be combined, the signal which can be attested can be transmitted and it is attested when it is the utilization whose control transaction of this does not need to access that radiotelephony holder's credit line, and when only authentication is important (for example, when unlocking that home garage door using radiotelephony), that control transaction will be performed.
[0008]
[Embodiment of the Invention] The gestalt of operation of this invention is illustrated in the following order, and is explained. It starts from the supply of the customer credit with which authentication and amount-of-money exchange become very important first, and explanation of the process of acquisition. Next, the process to which authentication accesses an indispensable home is explained. The process by which only the function of a command and control controls an important device like TV, for example is explained to the last. The following explanation is given by taking up the protocol used for a cellular phone and a cellular phone. However, when this invention is contrasted with other radiotelephony, it is still larger than the case of utilization of a cellular phone, for example. [of his understanding here]
[0009] 1. In a credit supply current, the process which supplies a customer credit is the considerably common actuation. For example, an organization like a bank provides a customer with a credit, this customer is supplied with a credit card, and this customer purchases goods and a screw using this credit card. If goods and service are purchased, it will be charged to this customer's card, this organization will send a description to this customer at the deadline for an invoicing cycle, and this customer will offset the credit with which it supplied that organization by the end of the payment date. Although it is natural, those who ask for acquisition of a credit card need to find the organization which supplies this credit. By the way, although it is not an especially difficult failure for many people to find the organization which supplies a credit, the following point attracts attention.
[0010] It attracts attention that it has much those who already have two or more communication

link business objects (local exchange service, long-distance communication link business object, cel communication link business object) and loan relation as for the customer of a credit. The problem which cannot use this diffused relation for supplying a general customer credit here, or asks that propriety arises. Since people who are carrying the cellular phone are becoming a large number, if this relation is used and it can process together with a credit card, to be sure, it is convenient. Arrangement and the process of explaining below offer this function. Although a cellular phone 10 is shown in drawing 1 , this is used in order to radiocommunicate with a base station 20. A base station 20 communicates with the credit center 40, and the credit center 40 communicates with a contractor's device 30. Moreover, a base station 50 also communicates with the credit center 40.

[0011] Although the cellular call-service provider who operates the credit center 40 and base stations 20 and 50 may belong to the same organization, it is not necessary to restrict to it. It is usual that the credit center 40 is a billing handling category in the organization which provides that user with this cellular call service. For example, the following case is assumed. A base station 20 belongs to the cellular call-service provider A, and a base station 50 belongs to the cellular call-service provider B, and the right holder of a cellular phone 10 has privity of contract with the cellular call-service provider B. Furthermore, the credit center 40 is made into the cellular call-service provider's B billing handling device. Moreover, a channel 21 is a channel which combines a device 30 with the credit center 40, and is the channel of a cable or wireless.

[0012] If authentication of an insurance guarantee can be acquired, since it is the communication link between a device 30 and the credit center 40, an either usual protocol can be used. The fundamental transaction about the case where a customer credit is acquired charges the amount of money chosen as the cellular phone 10 in the credit center 40 at the account of pair Perilla frutescens (L.) Britton var. crispa (Thunb.) Decne., and a contractor notifies this contractor of having obtained the benefit from this accounting to this radiotelephony holder's account. however, this comes out in the premise that a cellular phone 10 is in a right customer's hand. Since it is simple, when a query is in the justification of the possessor of this cellular phone, the protocol which requires it is not described here. The case of utilization, such as a customer's personal identification code and voice authentication, can be mentioned to this.

[0013] However, it may be said that recognizing here offers the guarantee whose both of that customer and contractor receive the profit of this supply credit in one in these technical problems. Another technical problem is offering this interaction by the approach by which insurance's was guaranteed that neither this customer nor its contractor gets disadvantageous profit. Still more nearly another technical problem is offering this interaction so that a third party's may not get disadvantageous profit by this communication link and a profit's may be obtained again. Although these objects show the example of the following patent made into an illustration here to drawing 2 here where it considers as reference, they are realized by the protocol. it -- United States patent No. 5,204,902 and Reeds ** -- refer to issuance on April 20, 1993. This Reeds's and others patent is described briefly. Here, there are the following in each cellular phone.

[0014] That is, there is digital string data of "common restricted data" (SSD), this is drawn from association of hash processing of a secret key (A-KEY), and there is that cellular phone device number (ESN) further, and there is that cellular phone allocation number (MIN1), random string data is one of those which each cellular phone has further, and the organization where this cellular telephone user has business relation chooses this as them. As an example of representation, this organization has the privity of contract which pays accounting which it is a

cellular call-service provider, and this cellular call-service provider and this customer "signed", that is, was produced. A cellular call-service provider is usually limited to the geographical area of specification [the area].
[0015] This area is that customer's "home" cellular call-service geographical area (home CGSA). The home CGSA of a cellular phone 10 presupposes that it is a base station 50 on account of explanation. The base station 20 of a cel where a cellular phone 10 exists presupposes that he is the "visiting place" host CGSA. This SSD train is divided into the SSDA train of two trains, and a SSDB train. This SSDA train is used for authentication and a SSDB train is used for communication link codes. Next, actuation explains. Each cel of a cel communication network is served by base station like (base stations 20 and 50). this base station -- being certain -- it chose -- although broadcast of the random sequence (RAND) is repeatedly carried out at a rate -- a security enhancement sake -- comparatively -- frequency -- many (for example, duration time of a cel call of most more frequently) this RAND is changed.
[0016] If a power source is put into the cellular phone which is in a certain cel, this RAND sequence is received, and that cel will be told about itself and will be answered (a cellular phone 10 receives RAND which a base station 20 transmits). This is a registration process and is shown by the lines (process) 11, 12, and 13 of drawing 2 . Processes 11, 12, and 13 are explained still more concretely. This cellular phone connects that ESN train and MIN1 train with that SSDA train and RAND train, carries out hash processing of the obtained string data, and acquires that AUTHR train. Next, this cellular phone transmits that AUTHR train to that base station with a RAND train, an ESN train, and MIN1 train for a check.
[0017] Although it swerves from explanation here, the reason for transmitting this RAND signal is that that base station has changed that RAND between the times of the time of a cellular phone 10 receiving RAND and its base station receiving AUTHR, this is an option, because it is because that base station can memorize the RAND train of that last easily. This base station opts for the discernment which detects this ESN train and MIN1 train and by which that cellular phone was asserted from here, and discernment of that home CGSA. Although it swerves, in order to identify this home CGSA, explanation needs to apply an algorithm to this ESN train and MIN1 train, or needs to refer for it to a database.
[0018] Although a base station 20 is this home CGSA and this is a base station 50 in the example of drawing 1 , hash processing of the string data which will receive this SSD train from now on, and might be combined with that RAND train and ESN train, and MIN1 train in this SSDA train is carried out, and the AUTHR train of that version is acquired. Next, this base station compares the AUTHR train of that version with the AUTHR train of that receiving version. Coincidence of these two string data determines the cellular phone as a right thing. In order that it may be transmitted to that cellular phone from this base station and "O.K." signal (line 13) may communicate further to this, the information about the specific frequency which this cellular phone needs to use is included.
[0019] If registered by this handling base station, although this cellular phone can start a call, this will be performed in the process which connects with other string data that call-ed telephone number that exists at least. Namely, as for this cellular phone, a new AUTHR train can also transmit further MIN3 train which is the information on that called party with that RAND train and ESN train, and MIN1 train. This new AUTHR train is acquired from RAND, ESN, MIN1 and MIN3, and hash processing of connection of SSDA (it is because there is no call which does not illustrate to drawing 2 , because is made into a third party). Once a dialogue with this base station is set up, if a actual information communication link is a request, it can progress by being

enciphered by SSDB.
[0020] In order to hold security furthermore, although this base station can require a reconfirmation certificate at any time, this is performed like said initial registration. Next, it returns to the technical problem which obtains a customer credit to the holder of the cel telephone 10. it is the need, in order to supply a credit and to charge this user's account in the credit center 40 -- the following step is most contained in a fundamental protocol.
(A) They are the required information about that account that communicates with the credit center 40 and charges it, the step which offers the total amount of money which charges that account, and the step which notifies returning that demand total amount of money to this contractor, and considering as a claim by the (B) contractor's device 30. It is convenient, if a step can furthermore be added, for example, the following term can be guaranteed.
[0021] It can mention guaranteeing not adding [which guarantees that return / which guarantees charging that offer credit to a right account / that demand total amount of money to a right contractor further, and it considers as a claim] the present or future damage to the credit center 40 or the user of a cellular phone 10 by the trespasser further again at this contractor etc. A detail protocol with the following step is shown as an example of the simple form.
(A) Although this contractor offers a code peculiar to that customer, this is a characteristic code which identifies this contractor in the credit center 40 (line 18 of drawing 2).
[0022] (B) This customer adds a matter like the example of a degree to a cellular phone 10. For example, it is a prefix as shown in "an asterisk and 9", is that contractor's ID code further, and is the total amount of money which needs to charge this customer's account further, needs to return to that contractor, and needs to be made into a claim. This forms MIN2 train.
(C) A cellular phone 10 is registered previously in a base station 20, and the data of a step (B) are inputted into that buffer, a that "transmitting" command is answered, and that MIN2 train, a RAND train, an ESN train, MIN1 train, and an AUTHR train are transmitted, however this AUTHR train is acquired from RAND, ESN, MIN1 and MIN2, and hash processing of connection of SSDA (line 14 of drawing 2).
[0023] (D) A base station's reception of this transmit information admits being what this is not usually a call (from for example, that "asterisk and 9" train), and is going to arrive at the credit center 40. It is answered, the credit center 40 is contacted and the related information is told. That is, this is the ESN and data of MIN1 and MIN2 (line 17 of drawing 2). It guarantees effectively that the Challenge Handshake Authentication Protocol of a base station 20 is a telephone corresponding to [in fact] the ESN and MIN1 which received in a cellular phone 10, therefore the credit center 40 is located in the location which deserves that the customer of MIN1 gets a credit, or asks for the right or wrong.
[0024] (E) If the credit center 40 determines that it needs to supply radiotelephony 10 with a credit, further probably as for this credit center, an acknowledgement code will be transmitted to a contractor's device 30 also like that cellular phone (lines 15 and 16 of drawing 2). The transaction of this request is successfully ended by reception of this acknowledgement. Actual copy **** of this credit to this customer's credit account is performed like usual, and this can change the tariff charge rate to a cellular phone 10, and can also perform it so that it may be carried out with "900 Service."
[0025] It is that this contractor needs to provide this customer with that code with the protocol of disclosure above in a point somewhat troublesome [one], and it is expected that an error arises if this step is performed by voice communication. It is because the process which a little thing for which the credit center 40 needs to contact a contractor's device is inconvenience, because this

needs utilization of the database which translates this contractor's code into the telephone number (usually), and sets up a communication path takes time amount further further again. However, these faults are conquered in the modification to which slight deformation, for example, this contractor, is rather another path, and he contacts the credit center 40, and the modification in which this contractor transmits that identification code to that credit center electronically.
[0026] Although it is natural, it is necessary to link the communication link between the radiotelephony 10 through a base station 20, and the credit center 40 with the communication link between a contractor 30 and the credit center 40 (for the purpose of being related). This link can be set up by that contractor that has agreed on the activity of the selected transaction password (TP train), and this customer. It seems that this string data shall be random, and shall be transitional, for example, shall merely be used only at once. This TP train can be inputted instead of this customer being that contractor's ID code, it can be transmitted to a base station 20, and that contractor can use the same TP for a communication link of a contractor with the credit center 40.
[0027] This TP train can be communicated from that contractor with voice to this customer, and this customer can insert this code in that cel telephone. Risk of a neighboring cellular phone joining this communication link accidentally, undertaking that credit amount of money, and considering as liability by this, is abolished. Since this TP train is merely used only at once, a trespasser does not have that value, and it is that an error at this step only makes that transaction go wrong clearly. When this arises, this customer and its contractor can reinput and retry this TP train (or a different TP train). Also when based on this deformation protocol, although that telephone communication is a front passage, it has the next point of difference here.
[0028] It contacts that credit center, clarifies an identity, and offers this TP train, and, in a suitable case, this contractor's device receives acknowledgement or authorization from that credit center. In order that the credit center 40 may help to link TP train which this contractor offered to the communication link by radiotelephony 10, it is convenient that a contractor's device 30 contains ESN and MIN1 of radiotelephony 10. This protocol is shown in drawing 3 . Although it is natural, a device 30 needs to receive the information on ESN and MIN1 from radiotelephony 10, and this can realize it with the receiver 31 which accompanies a device 30. It is possible that the customer who can use this receiver as a low sensibility receiver, because purchases that goods and service is in the neighborhood of this receiver, and this contractor wishes not to receive the transmission from an adjoining cellular phone again.
[0029] Reception of only a right cellular phone can be guaranteed by the approach except using a low sensibility receiver. For example, it can set so that all reception from a cellular phone that does not transmit this TP train for the receiver of a device 30 may be rejected. Or although a device 30 can have the metal shroud 32 around an antenna 31, however inserts the antenna of radiotelephony 10 here, an antenna 31 receives only the signal by this. If a receiver 31 is introduced into a device 30, however the communication link between the unrelated telephone 10 and a base station 20 may not surely carry out or there may be, it is not necessary to carry out directly. That is, a device 30 catches transmission of radiotelephony 10, whatever the data for which it asks, adds it, and does = (using pass 22 of drawing 1) transmission of this joint information through a base station 20 to the credit center 40.
[0030] Or a device 30 can bypass a base station 20, can transmit the data to the credit center 40 directly, and a preprocessor 42 receives the data and it emulates the registration process of a base station 20 here. As shown in drawing 4 , a contractor's device 30 acquires the RAND train from a preprocessor 42, and transmits it to radiotelephony 10. This contractor can transmit that TP train

to the user of radiotelephony 10 simultaneously. Radiotelephony 10 generates the following string data. There are that transaction password train (TP), an ESN train, and MIN1 train, and although it is an option, there is MIN2 train in this, and there is an AUTHR verification train (that TP train is embedded in this AUTHR train) in it further.
[0031] Next, a device 30 transmits this information to a preprocessor 42, and, probably adds that RAND train to this TP train, its total amount of money, its ID code, and a pan. Although a preprocessor 42 checks the justification of the user who demands a credit, it analyzes this AUTHR train to other data which the device 30 transmitted, and it performs it, supplies a credit, or determines that right or wrong. next, this decision -- a device -- 30 HE, although it is an option further, it is transmitted to radiotelephony 10. It can carry out by the ability of this contractor providing that customer with print-out, and this customer can sign this print-out according to a request, and a check with the document of the amount of money which charges this customer's account can be considered as backup verification of this accounting. By drawing 1 , equipment 33 shows this printer.
[0032] The device is completely the usual device [hardware / required for the system shown in drawing 1]. For example, a cellular phone 10 is also the usual cellular phone, and base stations 20 and 50 are the usual base stations similarly. As for this contractor's device, it being necessary to carry out by being a still easier receiver, or it is resemblance at the receiver of a base station 20 is only only distinguishing an input signal so that priority's may merely be given to a right input signal by reception of a signal. In this case, it is expected that the cellular phone of the customer who asks for purchase will 2-double-approach at least compared with the following cellular phone which approached most to that contractor's receiver. A shroud 32 is an effective thing which makes an error small at such distinction.
[0033] Then, the distinction based on the power to input is easy, and effective. However, such [again] distinction can remember that it can carry out only by checking that the TP train is included in the communication link from a cellular phone 10. It is necessary to embed from this at AUTHR and, and that cellular phone needs to output this TP train to "the free space which is not although interrupted." A means to add information to a contractor's device 30 at those received data in addition to this receiver, and to transmit this data to the credit center 40 is required. Such a device is the usual PC, or it can correct by specific hardware arrangement, and is low also in respect of a price also in respect of various functions, and can be realized now easily.
[0034] It can use by any class of printer ordinarily used for the printer about the usual credit card here now. About the credit center 40, this is office which serves as a communication link and a main role of a database in almost all cases, and does not differ from a current cellular phone provider's business office so.
[0035] 2. -- the home feedback above -- after shopping like the example which goes out privately, the holder of a cellular phone asks for access to the home, and asks for unlocking of a garage door under control of the same cellular phone. Here, it is not necessary to apply the credit center 40 for this object because, and a credit is not supplied (in accounting which it corrects, for example, this control transaction is performed by that base station, and is undertaken to that contribution, naturally, it excepts). The task which described the outline above is only the example of control of one garage door unlocking machine, and although it is not a requirement, it also has the example in which a communication link is included further as follows. In the example of a gestalt of communicative implementation, as for a garage door unlocking machine, a decode means is added with a cellular phone receiver.

[0036] Next, actuation explains. This garage door unlocking machine can be registered in that cellular phone base station, and this base station can incorporate that SSDA train and SSDB train there. Although this base station communicates with that garage door unlocking machine by the guaranteed method and this of the main point is almost the same as that of the case of other cellular phones, a point of difference is only the one direction communication link to a garage door receiver from this base station. If this cellular phone 10 wants to make that garage door unlocked, when wanting, it is required that it should be made to call to this garage door receiver in that base station, and series-of-commands data should be transmitted to that receiver. The following are one of those which are included in this data stream.
[0037] there is a random number (RANDX) in it -- having -- the holder of this cellular phone -- " -- it is devoted -- having -- " -- hash processing of this random number is carried out by the key (B-KEY) (are that TP train and a transaction password and was accumulated to this transaction) further in the cel telephone 10 in **. As mentioned above, there is a decode means in this receiver and this is a decode means to collect the string data which carried out hash processing by that B-KEY. When this decode random number is equivalent to the random number received in "the free space which is not although interrupted", that garage door is unlocked. This protocol is shown in drawing 5 , and lines 11, 12, and 13 show that registration process here, as drawing 2 was described.
[0038] It turns out that the protocol with which these cellular phones differ for a while by drawing 5 from the protocol of the usual telephone association is followed here. That RANDX train and B-KEY (RANDX) train are promptly added instead of waiting for the display to which this called party telephone number (MIN3) was only transmitted and which this called party specifically answered from that base station. This is easily performed by choosing this with this cellular phone, although the RANDX train which a user supplies to the sequences which this cellular phone can recognize easily (it reaches, otherwise does not correspond to effective string data), "8", and rightness continues. [for example,] Or although a cellular phone 10 is thinking, this MIN3 signal is transmitted and the remainder of that sequence is transmitted for a clear two SENDO signal to waiting and a degree.
[0039] In the example of a gestalt of the operation which does not include a communication link, this cellular phone base station operates with the still more nearly following semantics. That is, shortly after this cellular phone has a dialog with that base station automatically and turns on this cellular phone, notice is submitted itself and it is registered. For better or worse, if it puts in another way, if this cellular phone is turned on, notice will be itself submitted to that base station, and it will register with it. This activity does not usually generate accounting to that cellular phone holder's credit account. It is this object to unlock this garage door without the help from that base station in the example of a gestalt of the operation which does not include a communication link beyond this registering point.
[0040] Although this is attained by many approaches, the following point is surely required for it. The signal transmitted to this base station where it follows "O.K." signal of a line (drawing 5) 13 needs to be what is not understood in this base station. On the contrary, this garage door receiver needs to be aligned with that transmission from that cellular phone, and that transmission needs to understand it. This can be attained like the example of a degree. For example, although this garage door receiver is "O.K." signal of that base station, however the signal directed that this operates on a specific frequency to this cellular phone, this transmission is monitored and it can realize. Next, this receiver can be itself aligned with that same frequency, and can catch transmission of this cellular phone.

[0041] If a cellular phone 10 transmits the signal of the line 25 of drawing 5 next as shown in drawing 6 , this receiver will monitor it, it will be decoded and that garage door will answer there. or [MIN3 being string data which the base station does not recognize, or deleting AUTHR in such an example of a gestalt of operation,] -- or it only changes and refusal is made to cause by the base station Or if the "8" sequence is inserted in a cellular phone 10, it can align with the fixed appeal frequency used for registration itself. This garage door unlocking machine can be aligned with such implementation fixed in that appeal frequency. Said example of garage door unlocking is an example, and can mention other control utilization, for example, unlocking of an automobile door or a house, and an activating alarm, and these are also included by the technical range of this invention here.
[0042] 3. If it can access to the home of control ****** as a request, the holder of a cellular phone 10 can ask for control of various devices. It is not that security has an interest like [in said utilization of two examples] in such utilization. It is desirable not to include this base station in such control utilization from a viewpoint of a public policy further again. In the case of the latter, it can carry out only by changing the clock frequency of this cellular phone into the band which is not covered by this base station. Next, actuation explains. It operates on the frequency as which the home controller base station of itself is located at each home, and this was chosen. In a switch or code "driven in", this cellular phone can be made into "home controller" mode, and this cellular phone has a dialog only with that home controller base station in this mode.
[0043] next, what kind of control can perform it also for allocation **** to it using the approach usual in this home controller base station. Although this authentication process can be performed as mentioned above, it is carried out to the bottom of control of this home controller base station. That is, this home controller base station can include the function which attests that cellular phone as a home controller based on the interaction of that request, does not need to restrict it to it, or can also carry out it selectively. For example, it is also possible to be able to change TV channel as a home controller using this cellular phone, therefore to ask for a certain security processing probably.
[0044] However, although it can also have a dialog that television signal supply origin again using this cellular phone, it is not necessary to ask for security here. Purchasing by such interaction is also possible, and even if the owner of a home controller makes a visitor use this home controller base station as a conduit tube and it does not care about it, it does not interfere. Arrangement of disclosure is shown in drawing 7 above, the home base station 60 is here, there are further various home controllers 61, this controls a device, there are television "set top box" 62, and there is television 63, and there is a means 64 by which it can have a dialog the goods [which were further advertised on this television] and/or supply origin of service in this device.
[0045] Although it is also possible to make such a means into a part of the set top books and this returns a signal to the supply origin (it illustrates) of the television signal, it is not necessary to restrict to it. What should be written in addition here does not restrict the above explanation of this invention to a cellular phone. Although the function of disclosure is above realizable with any wireless means of a class, it may be the utilization it is the case where such a means has suitable authentication capacity to utilization at hand, however a desired authentication function is not important or is completely above unnecessary like explanation. Although the various modifications of this invention can consider the above explanation about the example of 1 gestalt of operation of this invention if it is this contractor of this technical field, each of they is included by the technical range of this invention. In addition, the reference number indicated to the claim

is for an understanding with easy invention, and should not be interpreted as restricting the technical range.

DESCRIPTION OF DRAWINGS

[Brief Description of the Drawings]
[Drawing 1] It is drawing showing the arrangement which performs the system of this invention.
[Drawing 2] It is the flow chart showing the flow of the example of a protocol used for the system of this invention.
[Drawing 3] It is the flow chart showing the flow of the example of a protocol used for the system of this invention.
[Drawing 4] It is the flow chart showing the flow of the example of a protocol used for the system of this invention.
[Drawing 5] It is the flow chart showing the flow for guarantee control utilization.
[Drawing 6] It is the flow chart showing the flow for guarantee control utilization.
[Drawing 7] It is drawing showing home controller base station arrangement.
[Description of Notations]
10 Cellular Phone
20 Radiotelephony Base Station
21 Channel
22 Pass
30 Vendor Device
31 Receiving Set
32 Shroud
33 Printer
40 Credit Center
42 Preprocessor
50 Radiotelephony Base Station
60 Home Controller Base Station
61 Home Controller
62 Set Top Box
63 Television
64 Controller

[Translation done.]

(19)日本国特許庁（ＪＰ）　(12) **公開特許公報（Ａ）**　(11)特許出願公開番号

特開平8－96043

(43)公開日　平成８年(1996)４月12日

(51)Int.Cl.[6]	識別記号	庁内整理番号	ＦＩ	技術表示箇所
Ｇ０６Ｆ　17/60				
19/00				
Ｈ０４Ｑ　7/38				
			Ｇ０６Ｆ　15/ 21	３４０　Ｂ
			15/ 30	Ｃ

審査請求　未請求　請求項の数19　ＦＤ　（全 10 頁）　最終頁に続く

(21)出願番号　特願平7－264673

(22)出願日　平成７年(1995)９月20日

(31)優先権主張番号　３１０４４１

(32)優先日　1994年９月22日

(33)優先権主張国　米国（ＵＳ）

(71)出願人　390035493
エイ・ティ・アンド・ティ・コーポレーション
ＡＴ&Ｔ　ＣＯＲＰ.
アメリカ合衆国　10013－2412　ニューヨーク　ニューヨーク　アヴェニュー　オブ　ジ　アメリカズ　32

(72)発明者　ビー．ワーリング　パートリッジ
アメリカ合衆国，07931　ニュージャージー，ファー　ヒルズ，オーランド　ロード　900

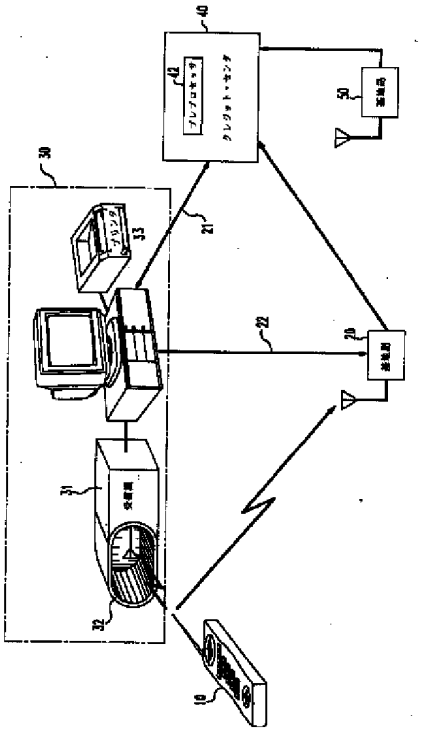
(74)代理人　弁理士　三俣　弘文

(54)【発明の名称】　アクション保証方法とクレジット提供配置

(57)【要約】

【課題】　認証されたトランザクション・コントローラのセル式電話を介し例えば、顧客にクレジットを提供する配置を提供する。

【解決手段】　本発明の実施の形態として、例えば、業者から商品またはサービスの購入にクレジットを求める顧客がそのセル式電話を起動し、このセル式電話をそのセル式電話サービス提供者の基地局に対して認証し、クレジットを得るよう結合の設定に進む。この被呼側電話番号に対応する通常の番号シーケンスとは異なる特有のシーケンスをセル式電話サービス提供者に送信してクレジットを得る。このシーケンスには業者のＩＤコードと所望クレジット金額を含む。



1

【特許請求の範囲】

【請求項１】　（Ａ）通信用に設けた無線通信装置（１０）を起動する起動ステップと、

（Ｂ）この無線通信装置が発信する信号に基づきこの無線通信装置の識別を認証する認証ステップと、

（Ｃ）この無線通信装置によって許可された特定のアクションを実行するアクション実行ステップとを有することを特徴とするユーザのためのアクションを保証するアクション保証方法。

【請求項２】　前記（Ｂ）認証ステップは、前記無線通信装置を通信利用に使用する場合に前記無線通信装置が使用する登録プロトコルの少くとも一部に少くとも部分的に対応するプロトコルを使用することを特徴とする請求項１に記載の方法。

【請求項３】　前記（Ｂ）認証ステップは、前記無線通信装置を通信利用に使用する場合に前記無線通信装置が使用する登録プロトコルに少くとも部分的に対応するプロトコルを使用することを特徴とする請求項１に記載の方法。

【請求項４】　前記ユーザのための前記アクションは、前記ユーザにクレジットを供与するクレジット供与ステップであることを特徴とする請求項１に記載の方法。

【請求項５】　前記クレジット供与ステップは、通信サービスを前記無線通信装置に提供する通信サービス提供者によって行われることを特徴とする請求項４に記載の方法。

【請求項６】　前記クレジット供与ステップは、通信サービスを前記無線通信装置に提供する通信サービス提供者以外の通信サービス非提供者によって行われることを特徴とする請求項４に記載の方法。

【請求項７】　前記ユーザのための前記アクションは、特定の行先へ保証制御信号を送信する保証制御信号送信ステップであることを特徴とする請求項１に記載の方法。

【請求項８】　前記ユーザのための前記アクションは、行先へ制御信号を送信する制御信号送信ステップであることを特徴とする請求項１に記載の方法。

【請求項９】　前記行先はホーム・コントローラ基地局（５０）であることを特徴とする請求項８に記載の方法。

【請求項１０】　前記行先は、テレビジョン・セットへ信号を提供する信号提供者と対話するホーム・コントローラ基地局（６０）であることを特徴とする請求項８に記載に方法。

【請求項１１】　前記クレジット供与ステップは、トランザクション・パスワード部分列、クレジット金額部分列、ＩＤ部分列および検証部分列を含む列データをクレジット提供センタに送信するステップを有することを特徴とする請求項４に記載の方法。

【請求項１２】　無線電話を持ちおよびクレジット提供センタ（４０）と関係と持つ第１の当事者に第２の当事者の利益のためにクレジットを提供するクレジット提供配置において、

（Ａ）無線通信用に前記無線電話が使用する識別プロトコルと適合する識別プロトコルを使用し前記クレジット・センタに対し前記無線電話を識別する第１の手段と、

（Ｂ）前記第２の当事者の識別とクレジット合計金額を前記第１の手段によって識別された無線電話と関係付ける第２の手段と、

（Ｃ）前記クレジット・センタが前記第２の当事者に承認ステータスを通信する第３の手段を有することを特徴とするクレジット提供配置。

【請求項１３】　前記第１の手段と前記第２の手段と前記第３の手段の基本的要素は前記クレジット提供センタの制御下にあることを特徴とする請求項１２に記載の配置。

【請求項１４】　前記第１の手段はセルラ電話基地局とこのセルラ電話基地局と前記クレジット・センタ間の通信リンクを有することを特徴とする請求項１２に記載の配置。

【請求項１５】　前記第１の手段は前記クレジット・センタと通信するため前記第２の当事者の構内に送信装置（３０）を持つことを特徴とする請求項１２に記載の配置。

【請求項１６】　前記第２の当事者の構内の前記送信装置はセルラ電話基地局を介し前記クレジット・センタと通信することを特徴とする請求項１５に記載の配置。

【請求項１７】　前記第１の手段と前記第２の手段と前記第３の手段の基本的要素は前記第２の当事者の構内に配置することを特徴とする配置。

【請求項１８】　前記第１の手段はさらに前記無線電話と通信するため受信装置（３１）を有することを特徴とする請求項１７に記載の配置。

【請求項１９】　さらに、前記無線電話からの送信を他の無線電話からの送信から判別する手段を有することを特徴とする請求項１８に記載の配置。

【発明の詳細な説明】

【０００１】

【発明の属する技術分野】本発明は、無線電話に係り、特にこの無線電話の保持者のためのアクションを保証する無線電話の利用プロセスに関する。

【０００２】

【従来の技術】現在無線電話は専ら通信用に利用されている。一方ユーザのためのアクションを保証するためには次例のような別の装置が利用されている。例えば、赤外線方式の遠隔制御装置を利用してＴＶやＶＣＲなどを制御する。また家のキーを利用して家の中へ入ることを保証する。またクレジット・カードを利用して顧客クレジットを得る例などである。これらの活動をすべて“制御トランザクション”と分類することができる、という

のはこのユーザによって制御が行われある所望の結果または利益が得られるからである。

【０００３】これらトランザクションの中であるものは無料であって、例えば、自分の家に入ることを保証する例、ＴＶの無料チャネルの受信を制御する例、などを挙げるころができる。またあるトランザクションは有料であって、例えば、劇場に入ることを保証する例、視聴当たりの“ペイ”ＴＶチャネルを選択する例、顧客クレジットを得る例、などを挙げることができる。本発明の目的は下記の制御トランザクションに関する課題を解決するシステムを提供することであって次の通りである。

【０００４】

【発明が解決しようとする課題】ユーザにその無線電話を利用させ制御トランザクションを行わせるシステムおよび有料の制御トランザクションの場合にはこの制御トランザクションのコストをその無線電話サービス提供者または別の当事者に対しこの無線電話の保持者が持つクレジット口座に負わせるシステムの提供が望まれている。

【０００５】

【課題を解決するための手段】本発明は、無線電話を利用してユーザのためのアクションを保証しそれによって保証されたトランザクション・コントローラを形成する。この手順はこの無線電話を起動するとそれに係る認証プロトコルに基くものである。いったんこの無線電話が認証されてしまうと、制御コマンドがその無線電話によって（またはその無線電話によって有効に）発せられ、また必要に応じこの無線電話サービス提供者に対しクレジット合計金額をこの無線電話の保持者が持つクレジット口座に負わせるることを許可しそれに債務とする。

【０００６】顧客クレジットの受入れを求める利用の場合、例えば、商品やサービスの販売業者（以下単に業者と略す）からそれを購入するためクレジットを求める顧客は次のように行う。この顧客は、その無線電話を起動し、そのローカル基地局を通じてこの無線電話サービス提供者に対しこの無線電話を認証し、クレジットを得るため“対話”を確立するよう進む。クレジットは、特有のシーケンスつまりその被呼側電話番号に対応する通常番号シーケンスと異なるシーケンスとすることができるような特有のシーケンスを無線電話サービス提供者に送信して得られる。このシーケンスに含むものには、業者ＩＤコード（その販売業者を識別するもの）があり、さらに当然のことであるが、所望クレジット金額があり、さらにまた他の情報、例えば、購入アイテムや受けるサービスなどの情報を挙げることができる。

【０００７】本発明の実施の別の形態では、この業者の無線受信装置がその基地局へ送信される情報を傍受し、この業者と所望クレジット金額に関する情報を追加し、この情報をそのクレジット提供組織、すなわちこの無線電話保持者の口座を有する組織、へ送信する。このクレジット提供組織との通信は無線通信または有線通信を通じ行うことができる。このクレジットに対する要求が適切と判断されると、この業者にメッセージを送信し、クレジットの供与を許可し、このトランザクションは成功裡に終了する。この制御トランザクションがその無線電話保持者のクレジット・ラインをアクセスする必要がないような利用の場合、また認証のみが重要であるような場合、例えば、無線電話を利用してそのホーム・ガレージ・ドアを開錠するような場合、無線電話基地局のランダム信号を結合し認証可能な信号を送信することができ、認証されると、その制御トランザクションを行う。

【０００８】

【発明の実施の形態】本発明の実施の形態を次の順序で例示し説明する。先ず認証と金額交換が非常に重要となる顧客クレジットの供与と取得のプロセスの説明から開始する。次に認証が不可欠であるホームにアクセスするプロセスを説明する。最後にコマンドと制御の機能だけが重要である例えば、ＴＶのような機器を制御するプロセスを説明する。以下の説明はセルラ電話とセルラ電話に利用されるプロトコルを取上げ行う。ただしここで理解する必要があるのは本発明は、他の無線電話に対比すると、例えば、セルラ電話の利用の場合よりさらに広いものである。

【０００９】１．クレジット供与

現在では顧客クレジットを供与するプロセスはかなりありふれた動作である。例えば、銀行のような組織が顧客にクレジットを提供し、この顧客にクレジット・カードを供与し、この顧客はこのクレジット・カードを使って商品やビスを購入する。商品やサービスを購入すると、この顧客のカードに対し課金され、代金請求サイクルの最終期限にこの組織がこの顧客に明細書を送付し、支払い期日中にこの顧客はその組織にそれが供与したクレジットの相殺をする。当然のことであるが、クレジット・カードの取得を所望する者はこのクレジットを供与する組織を見付ける必要がある。ところでクレジットを供与する組織を見付けることは多数の人々にとって特に難しい障害ではないが、次の点が注目される。

【００１０】それはクレジットの顧客はすでに複数の通信事業体（市内交換局サービス、長距離通信事業体、セル通信事業体）と貸借関係をすでに持っている者が多いということが注目される。ここで一般顧客クレジットを供与するのにこの普及している関係を利用することができないかその可否を問う問題が生ずる。セルラ電話を携帯している人々が多数になってきているのでこの関係を利用しクレジット・カードで一緒に処理できれば確かに好都合である。この機能を以下に説明する配置とプロセスが提供する。図１にセルラ電話１０を示すがこれは基地局２０と無線通信するため用いられる。基地局２０はクレジット・センタ４０と通信し、またクレジット・セ

5

ンタ４０は業者の機器３０と通信する。また基地局５０もクレジット・センタ４０と通信する。

【００１１】クレジット・センタ４０と基地局２０、５０を動作させるセルラ電話サービス提供者が同一組織のものである場合があるが、それに限る必要はない。クレジット・センタ４０はこのセルラ電話サービスをそのユーザに提供する組織の中の料金請求取扱部門であるのが通常である。例えば次の場合を仮定する。基地局２０はセルラ電話サービス提供者Ａに属し、基地局５０はセルラ電話サービス提供者Ｂに属し、およびセルラ電話１０の正しい保持者はセルラ電話サービス提供者Ｂと契約関係を持つ。さらにクレジット・センタ４０はセルラ電話サービス提供者Ｂの料金請求取扱機構とする。またチャネル２１は機器３０をクレジット・センタ４０に結合するチャネルであって有線または無線の通信路である。

【００１２】安全保証の認証を得ることができると、機器３０とクレジット・センタ４０間の通信のためいずれか通常のプロトコルを用いることができる。顧客クレジットを取得する場合に関する基本的トランザクションは、セルラ電話１０に対しその口座にクレジット・センタ４０で選択した金額を課金し、この無線電話保持者の口座に対するこの課金から業者は受益を得ていることをこの業者に通知する。ただしこれはセルラ電話１０が正しい顧客の手にあるという前提においてである。簡略のため、このセルラ電話の所持者の正当性に疑問がある場合にそれが係るプロトコルについてはここでは述べない。これには、例えば、顧客のパーソナル識別コードや音声認証などの利用の場合を挙げることができる。

【００１３】しかしここで認識することは、これら課題の中の一つにこの供与クレジットの利益をその顧客と業者の両者が受ける保証をするということがある。別の課題はこの顧客もその業者も不利益を得ないよう安全が保証された方法でこのインタラクションを提供することである。さらに別の課題はこの通信によって第三者が不利益を得ないようまた利益を得るようこのインタラクションを提供することである。これらの目的は、ここに引例とする下記特許例を参照とする、ここでは図２に示すが、そのプロトコルによって実現される。それは、米国特許第５、２０４、９０２号、Reeds ら、１９９３年４月２０日発行、を参照のこと。このReedsらの特許を簡単に述べる。ここでは各セルラ電話には下記のものがある。

【００１４】すなわち、各セルラ電話の持つものには、“共用秘密データ”（ＳＳＤ）のディジタル列データがあってこれは秘密キー（Ａ－ＫＥＹ）のハッシュ処理の結合から導かれたものであり、さらにそのセルラ電話装置番号（ＥＳＮ）があり、またそのセルラ電話割当番号（ＭＩＮ１）があり、さらにランダム列データがあってこれはこのセルラ電話ユーザがビジネス関係を持つ組織が選択するものである。代表例として、この組織はセルラ電話サービス提供者であってこのセルラ電話サービス提供者とこの顧客が“署名”し、つまり生じた課金を支払う契約関係を持つものである。セルラ電話サービス提供者はその地域が特定の地理的エリアに通常限定される。

6

【００１５】このエリアはその顧客の“ホーム”セルラ電話サービス地理的エリア（ホームＣＧＳＡ）である。説明の都合上、セルラ電話１０のホームＣＧＳＡは基地局５０であるとする。セルラ電話１０が存在するセルの基地局２０は“訪問先”ホストＣＧＳＡであるとする。このＳＳＤ列は２個の列のＳＳＤＡ列とＳＳＤＢ列に分けられる。このＳＳＤＡ列は認証用に用い、ＳＳＤＢ列は通信暗号用に用いる。次に動作で説明する。セル通信網の各セルは（基地局２０、５０）のような基地局によってサービスされる。この基地局はある選択した繰返しレートでランダム・シーケンス（ＲＡＮＤ）を同報通信するが、セキュリティ増強のため比較的頻度多く（例えば、大部分のセル呼出の継続時間よりもっと度々）このＲＡＮＤを変更する。

【００１６】あるセル内にいるセルラ電話に電源を入れると、このＲＡＮＤシーケンスを受信しそしてそのセルに自分自身を知らせて応答する（セルラ電話１０は基地局２０が送信するＲＡＮＤを受信する）。これは登録プロセスであって図２のライン（プロセス）１１、１２、１３で示される。プロセス１１、１２、１３をさらに具体的に説明する。このセルラ電話はそのＥＳＮ列とＭＩＮ１列をそのＳＳＤＡ列とＲＡＮＤ列とに連結し、得られた列データをハッシュ処理してそのＡＵＴＨＲ列を得る。次にこのセルラ電話はそのＡＵＴＨＲ列をＲＡＮＤ列とＥＳＮ列とＭＩＮ１列とともにその基地局へ確認のため送信する。

【００１７】ここで説明はそれるが、このＲＡＮＤ信号を送信する理由は、セルラ電話１０がＲＡＮＤを受信した時とその基地局がＡＵＴＨＲを受信する時との間にその基地局がそのＲＡＮＤを変更したことがあるからであり、ただしこれはオプションであってというのはその基地局はその最後のＲＡＮＤ列を容易に記憶することができるからである。この基地局はこのＥＳＮ列とＭＩＮ１列を検出してここからそのセルラ電話のアサートされた識別とそのホームＣＧＳＡの識別を決定する。説明はそれるが、このホームＣＧＳＡを識別するためにはアルゴリズムをこのＥＳＮ列とＭＩＮ１列に適用する必要があるかまたはデータベースに照会する必要がある。

【００１８】基地局２０はこのホームＣＧＳＡ、ただしこれは図１の例では基地局５０であるが、これからこのＳＳＤ列を受信しこのＳＳＤＡ列をそのＲＡＮＤ列とＥＳＮ列とＭＩＮ１列と結合し得られた列データをハッシュ処理してそのバージョンのＡＵＴＨＲ列を得る。次にこの基地局はそのバージョンのＡＵＴＨＲ列をその受信バージョンのＡＵＴＨＲ列と比較する。これら２個の列

データが一致すると、そのセルラ電話は正しいものと決定される。“ＯＫ”信号（ライン１３）がこの基地局からそのセルラ電話に送信されこれにはさらに通信するためにこのセルラ電話が使用する必要がある特定の周波数に関する情報を含む。

【００１９】この取扱基地局によって登録されると、このセルラ電話は呼出を開始することができるがこれは少なくともあるその被呼電話番号をその他の列データに連結するプロセスで行われる。すなわち、このセルラ電話は、その被呼側の情報であるＭＩＮ３列を、そのＲＡＮＤ列とＥＳＮ列とＭＩＮ１列とともに、さらに新規ＡＵＴＨＲ列も、送信することができる。この新規ＡＵＴＨＲ列はＲＡＮＤ、ＥＳＮ、ＭＩＮ１、ＭＩＮ３およびＳＳＤＡの連結のハッシュ処理から得られる（図２には図示せず、というのは第三者にされる呼出がないためである）。いったんこの基地局との対話が設定されてしまうと、実際の情報通信は、所望ならば、ＳＳＤＢで暗号化され、進むことができる。

【００２０】さらにセキュリティを保持するためこの基地局は何時でも再認証を要求できるがこれは前記初期登録と同様に行われる。次にセル電話１０の保持者に対し顧客クレジットを得る課題に戻る。クレジットを供与しクレジット・センタ４０でこのユーザの口座に課金するために必要な最も基本的プロトコルには次のステップが含まれる。

（Ａ）クレジット・センタ４０と通信しそれに課金するその口座に関する必要情報とその口座に課金する合計金額を提供するステップと、（Ｂ）業者の機器３０によってこの業者にその要求合計金額を帰し債権とすることを通知するステップである。さらにステップを追加して例えば、次項を保証することができれば好都合である。

【００２１】それは正しい口座にその提供クレジットを課金することを保証する、さらに正しい業者にその要求合計金額を帰し債権とすることを保証する、さらに侵害者によって現在または将来の損害をこの業者に、またクレジット・センタ４０に、またはセルラ電話１０のユーザに、加えないことを保証する、などを挙げることができる。その単純な形の一例として、次のステップを持つ詳細プロトコルを示す。

（Ａ）この業者はその顧客に特有のコードを提供するがこれはクレジット・センタ４０にこの業者を識別する特有のコードである（図２のライン１８）。

【００２２】（Ｂ）この顧客は次例のような事項をセルラ電話１０に加える。例えば、“星印と９”のような接頭部であり、さらにその業者のＩＤコードであり、さらにこの顧客の口座に課金しその業者に帰し債権とする必要がある合計金額である。これがＭＩＮ２列を形成する。

（Ｃ）セルラ電話１０は、基地局２０で先に登録され、またステップ（Ｂ）のデータがそのバッファに入力されており、その“送信”コマンドに応答してそのＭＩＮ２列、ＲＡＮＤ列、ＥＳＮ列、ＭＩＮ１列およびＡＵＴＨＲ列を送信する，ただしこのＡＵＴＨＲ列はＲＡＮＤ、ＥＳＮ、ＭＩＮ１、ＭＩＮ２およびＳＳＤＡの連結のハッシュ処理から得られる（図２のライン１４）。

【００２３】（Ｄ）基地局がこの送信情報を受信すると、（例えば、その“星印と９”列から）これは通常呼出ではなくクレジット・センタ４０に達しようとしているものであることを認める。それに応答してクレジット・センタ４０が接触されその関連情報が伝えられる。すなわちこれは、そのＥＳＮとＭＩＮ１とＭＩＮ２のデータである（図２のライン１７）。基地局２０の認証プロトコルはセルラ電話１０が実はその受信したＥＳＮとＭＩＮ１に対応する電話であることを有効に保証し、したがってクレジット・センタ４０はＭＩＮ１の顧客がクレジットを得るに値するかその正否を求める位置にある。

【００２４】（Ｅ）クレジット・センタ４０が無線電話１０にクレジットを供与する必要があると決定すると、このクレジット・センタは承認コードを業者の機器３０に、さらにおそらくそのセルラ電話にも同様に、送信する（図２のライン１５、１６）。この承認の受信でこの所望のトランザクションは成功裡に終了する。この顧客のクレジット口座に対するこのクレジットの実際の転記記帳は通常のように行われ、またこれは“９００サービス”で行われるように、セルラ電話１０に対する料金課金レートを変えて行うこともできる。

【００２５】以上開示のプロトコルで一つ少し厄介な点はこの業者はそのコードをこの顧客に提供する必要があることで、もしこのステップを音声通信で行うとエラーが生ずることが予想される。さらにまた、クレジット・センタ４０が業者の機器と接触する必要があることは少し不都合であり、というのはこれはこの業者のコードを（通常）電話番号に翻訳するデータベースの利用を必要とし、また通信パスを設定するプロセスがさらに時間を取るからである。しかしこれらの欠点は、僅かな変形、例えば、この業者がクレジット・センタ４０と、どちらかといえば別の経路で、接触する変形例、またこの業者がその識別コードをそのクレジット・センタに電子的に送信する変形例で克服される。

【００２６】当然のことであるが、基地局２０を介する無線電話１０とクレジット・センタ４０間の通信は、業者３０とクレジット・センタ４０間の通信と（関係しているという意味で）リンクする必要がある。このリンクは、選択したトランザクション・パスワード（ＴＰ列）の使用に合意したその業者とこの顧客によって設定することができる。この列データはランダムで過渡的な、例えば、ただ一度だけ使用するような、ものとすることができる。この顧客がその業者のＩＤコードの代わりにこのＴＰ列を入力し、それを基地局２０に送信し、その業者が同一ＴＰをクレジット・センタ４０との業者の通信

に利用することができる。

【００２７】このＴＰ列をその業者からこの顧客に音声で通信することができ、この顧客はこのコードをそのセル電話に挿入することができる。これによって近隣のセルラ電話が誤ってこの通信に加わりそのクレジット金額を負い債務とする危険をなくする。このＴＰ列はただ一度だけ使用されるので侵害者にその価値は無く、このステップでのエラーはそのトランザクションを明白に失敗させるだけに過ぎない。これが生ずる場合には、この顧客とその業者はこのＴＰ列（または異なるＴＰ列）を再入力し再試行することができる。この変形プロトコルによる場合もその電話通信は前の通りであるがここで次の相違点がある。

【００２８】それは、この業者の機器はそのクレジット・センタと接触し、身元を明らかにし、このＴＰ列を提供し、適切な場合、そのクレジット・センタから承認または許可を受信する。クレジット・センタ４０がこの業者が提供したＴＰ列を無線電話１０による通信にリンクするのを助けるため、業者の機器３０が無線電話１０のＥＳＮとＭＩＮ１を含むことは好都合である。このプロトコルを図３に示す。当然のことであるが、機器３０は無線電話１０からそのＥＳＮとＭＩＮ１の情報を受信する必要があってこれは機器３０に付随する受信機３１によって実現することができる。この受信機は低感度受信機とすることができる、というのはその商品やサービスを購入する顧客はこの受信機の近隣にいることが考えられまたこの業者は隣接するセルラ電話からの送信を受信しないことを所望する。

【００２９】正しいセルラ電話だけの受信を低感度受信機を利用する以外の方法で保証することができる。例えば、機器３０の受信機をこのＴＰ列を送信しないセルラ電話からの受信をすべて棄却するようセットすることができる。または機器３０が金属シュラウド３２をアンテナ３１の周囲に有することができ、ただしここに無線電話１０のアンテナを挿入するが、これによってその信号のみをアンテナ３１が受信するようにする。受信機３１が機器３０に導入されると、無縁電話１０と基地局２０間の通信が必ず行う必要はなく、またはどうあっても直接行う必要もない。すなわち、機器３０は無線電話１０の送信を捕え、所望するデータが何であれそれを付加し、この結合情報をクレジット・センタ４０へ基地局２０を介し〓（図１のパス２２を利用し）送信する。

【００３０】または、機器３０は基地局２０をバイパスして直接そのデータをクレジット・センタ４０へ送信することができここではプレプロセッサ４２がそのデータを受信し基地局２０の登録プロセスをエミュレートする。図４に示すように、業者の機器３０はプレプロセッサ４２からそのＲＡＮＤ列を得てそれを無線電話１０へ送信する。同時にこの業者はそのＴＰ列を無線電話１０のユーザへ送信することができる。無線電話１０は次の列データを生成する。これには、そのトランザクション・パスワード列（ＴＰ）、ＥＳＮ列、ＭＩＮ１列があり、またオプションであるがＭＩＮ２列があり、さらにＡＵＴＨＲ検証列（このＡＵＴＨＲ列にそのＴＰ列が埋め込まれている）がある。

【００３１】次に機器３０はこの情報をプレプロセッサ４２に送信し、このＴＰ列、その合計金額、そのＩＤコード、さらにおそらくそのＲＡＮＤ列、を加える。プレプロセッサ４２はクレジットを要求するユーザの正当性を確認するがそれは機器３０が送信した他のデータに対しこのＡＵＴＨＲ列を解析して行い、そしてクレジットを供与するかその正否を決定する。次にこの判断は機器３０へ、さらにオプションであるが無線電話１０へ、送信される。この顧客の口座に課金する金額の書面での確認はこの業者がその顧客にプリントアウトを提供し行うことができ、また所望に応じこのプリントアウトにこの顧客が署名しこの課金のバックアップ検証とすることができる。このプリンタは図１では装置３３で示す。

【００３２】図１に示すシステムに必要なハードウェアについてはその機器は全く通常の機器である。例えば、セルラ電話１０も通常のセルラ電話であり、また基地局２０、５０も同様に通常の基地局である。この業者の機器は単に基地局２０の受信機に類似のまたはさらに簡単な受信機であって、実施する必要があることはただ信号の受信で正しい入力信号を優先するよう受信信号を判別することだけである。この場合購入を所望する顧客のセルラ電話はその業者の受信機に対し最も近接した次のセルラ電話に比べ少くとも２倍接近していることが期待される。シュラウド３２はこのような判別にエラーを小さくする有効なものである。

【００３３】そこで入力する電力に基く判別は簡単で有効である。しかしまたこのような判別はそのＴＰ列がセルラ電話１０からの通信に含まれていることを単に確認するだけで実施可能であることを思い出すことができる。このことからＡＵＴＨＲに埋め込みかつ“遮るものの無い自由空間”にこのＴＰ列をそのセルラ電話が出力する必要がある。業者の機器３０にはこの受信機に加えてその受信データに情報を追加しこのデータをクレジット・センタ４０に送信する手段が必要である。このような機器は通常のＰＣでまたは特定のハードウェア配置でただし多機能の点でも価格の点でも低いもので、これで容易に実現することができる。

【００３４】ここでプリンタには通常のクレジット・カードに関しては現在普通に使用されているプリンタのいずれの種類でも利用することができる。クレジット・センタ４０に関しては、これはほとんどの場合通信とデータベースの中心役割となるオフィスであって現在のセルラ電話提供者のビジネス・オフィスとそう違わないものである。

【００３５】２．ホーム帰還

前記私的に出掛ける例のようなショッピングの後、セルラ電話の保持者はそのホームへのアクセスを所望し同じセルラ電話の制御下でガレージ・ドアの開錠を所望する。この目的のためにはクレジット・センタ４０が係る必要はない、というのはここではクレジットが供与されることはない（ただし、例えば、その基地局によってこの制御トランザクションが行われその寄与に対して負う課金の場合は当然除外する）。以上概要を述べたタスクは単に一つのガレージ・ドア開錠機の制御例であって必要条件ではないが下記のようにさらに通信が含まれる例もある。通信の実施の形態例では、ガレージ・ドア開錠機はセルラ電話受信機で解読手段が追加されたものである。

【００３６】次に動作で説明する。このガレージ・ドア開錠機をそのセルラ電話基地局で登録し、この基地局がそのＳＳＤＡ列とＳＳＤＢ列をそこに組込むことができる。要点は、この基地局は保証された仕方でそのガレージ・ドア開錠機と通信し、これは他のセルラ電話の場合とほとんど同様であるが、相違点はこの基地局からガレージ・ドア受信機への一方向通信のみということである。このセルラ電話１０がそのガレージ・ドアを開錠させたいと所望する場合、その基地局にこのガレージ・ドア受信機に呼出を行わせコマンド列データをその受信機に送信するように要求する。このデータ列に含むものに次のものがある。

【００３７】それには、乱数（ＲＡＮＤＸ）があってこれはこのセルラ電話の保持者によって“打込まれ”たもの（そのＴＰ列、トランザクション・パスワードで、このトランザクションに対するもの）であり、さらにセル電話１０に蓄積したキー（Ｂ－ＫＥＹ）でこの乱数をハッシュ処理したものである。前述のように、この受信機には解読手段があってこれはそのＢ－ＫＥＹでハッシュ処理した列データを回収する解読手段である。この解読乱数が“遮るものの無い自由空間”で受信した乱数に対応する場合、そのガレージ・ドアは開錠される。このプロトコルを図５に示し、ここでライン１１、１２、１３が、図２について述べたように、その登録プロセスを示す。

【００３８】ここでこのセルラ電話は、通常の電話結合のプロトコルからは図５で少し異なるプロトコルに従うことが分かる。具体的には、この被呼側電話番号（ＭＩＮ３）を単に送信しその基地局からこの被呼者が応答した表示を待つ代わりに、そのＲＡＮＤＸ列とＢ－ＫＥＹ（ＲＡＮＤＸ）列を直ちに追加する。これは、このセルラ電話が容易に認識できる（およびさもなければ有効な列データに対応しない）シーケンス、例えば、“８”、ただしさらにユーザが供給するＲＡＮＤＸ列が続くが、これをこのセルラ電話では選択することによって容易に行われる。または、セルラ電話１０は、考えられることであるが、このＭＩＮ３信号を送信し、クリアツーセンド信号を待ち、次にそのシーケンスの残部を送信する。

【００３９】通信を含まない実施の形態例では、このセルラ電話基地局はなお次のような意味を持って動作する。つまり、このセルラ電話はその基地局と自動的に対話しこのセルラ電話の電源を入れると直ちに自ら届出て登録する。換言すると、好むと好まざるとにかかわらず、このセルラ電話の電源を入れると、その基地局に自ら届出て登録する。この活動は、通常、そのセルラ電話保持者のクレジット口座に課金を生成しない。この登録点以上には通信を含まない実施の形態例ではその基地局からの手助け無しにこのガレージ・ドアを開錠することが本目的である。

【００４０】これは多数の方法で達成されるが次の点が必ず必要である。それは、（図５の）ライン１３の“ＯＫ”信号に続くこの基地局へ送信される信号はこの基地局には分からないものであることが必要である。逆に、このガレージ・ドア受信機はそのセルラ電話からのその送信に同調しその送信が分かる必要がある。これは次例のように達成することができる。例えば、このガレージ・ドア受信機がその基地局の“ＯＫ”信号、ただしこれはこのセルラ電話に特定の周波数で動作するよう指示する信号であるが、この送信を傍受して実現できる。次にこの受信機はその同じ周波数に自ら同調してこのセルラ電話の送信を捕えることができる。

【００４１】図６に示すように、次にセルラ電話１０が図５のライン２５の信号を送信すると、この受信機はそれを傍受し、それを解読し、そこでそのガレージ・ドアが応答する。このような実施の形態例では、ＭＩＮ３はその基地局が認識しない列データであって、またはＡＵＴＨＲを削除するかまたは単に変更してその基地局によって拒否を起こさせる。または、その“８”シーケンスをセルラ電話１０に挿入すると、登録用に用いる固定呼掛け周波数に自ら同調することができる。このような実現に、このガレージ・ドア開錠機はその呼掛け周波数に固定的に同調することができる。ここでガレージ・ドア開錠の前記例は一例であって他の制御利用、例えば、自動車ドアや家の開錠、アラーム起動を挙げることができ、これらも本発明の技術的範囲に包含される。

【００４２】３．制御拡張

そのホームへ所望通りアクセスできると、セルラ電話１０の保持者は種々の機器の制御を所望することができる。このような利用の場合にはセキュリティは、前記２例の利用の場合のような関心のあることではない。さらにまた公共ポリシーの観点からもこの基地局をこのような制御利用には含まないことが望ましい。後者の場合はこの基地局によってカバーされない帯域にこのセルラ電話の動作周波数を単に変更するだけで実施可能である。次に動作で説明する。各ホームにはそれ自身のホーム・コントローラ基地局があってこれが選択された周波数で動作する。スイッチまたは“打込んだ”コードによって

13

このセルラ電話を“ホーム・コントローラ”モードにすることができ、このモードではこのセルラ電話はそのホーム・コントローラ基地局とだけ対話する。

【００４３】次にこのホーム・コントローラ基地局は通常の方法を用いてそれにいかなる制御が割当られてもそれを実行することができる。この認証プロセスは前記のように行うことができるが、ただしこのホーム・コントローラ基地局の制御下に行われる。すなわち、このホーム・コントローラ基地局は、その所望のインタラクションに基づきホーム・コントローラとしてそのセルラ電話を認証する機能を含むことができ、ただしそれに限る必要はなく、または選択的にそれをすることもできる。例えば、ホーム・コントローラとしてこのセルラ電話を利用してＴＶチャネルを変えることができ、そのためにおそらくあるセキュリティ処理を所望することも可能である。

【００４４】しかしまたこのセルラ電話を利用してそのテレビジョン信号供給元と対話することもできるがただしここではセキュリティを求めなくてよい。このようなインタラクションによって購入を行うことも可能であってホーム・コントローラのオーナは訪問者にこのホーム・コントローラ基地局をコンジットとして利用させても気にしなくても差支えない。以上開示の配置を図７に示し、ここにはホーム基地局６０があり、さらに種々のホーム・コントローラ６１があってこれが機器を制御し、この機器には例えば、テレビジョン“セット・トップ・ボックス”６２があり、またテレビジョン６３があり、さらにこのテレビジョン上に広告された商品および／またはサービスの供給元と対話できる手段６４がある。

【００４５】このような手段をそのセット・トップ・ブックスの一部とすることも可能であってこれはそのテレビジョン信号の供給元（図示するが）へ信号を返送するが、またそれに限る必要もない。ここで付記すべきことは本発明の以上の説明はセルラ電話に限るものではない。いずれの種類の無線手段でも以上開示の機能を実現することができるが、ただしそれはこのような手段が手元の利用に対し適当な認証能力を持つ場合であって、しかし以上説明のように所望の認証機能が重要でなくまたは全く不要であるような利用の場合もある。以上の説明は、本発明の実施の一形態例に関するもので、この技術分野の当業者であれば、本発明の種々の変形例が考え得るが、それらはいずれも本発明の技術的範囲に包含される。尚、特許請求の範囲に記載した参照番号は発明の容易なる理解のためで、その技術的範囲を制限するよう解釈されるべきではない。

14

【００４６】

【発明の効果】以上述べたごとく、本発明によって、認証したトランザクション・コントローラで、例えば、セルラ電話を利用して顧客クレジットで金額交換を行い、またホーム・ガレージ・ドアを開錠させ、さらにテレビジョン広告の商品やサービスの対話に利用でき、有効な認証したトランザクション・コントローラを提供することができ、通信利用にさらに多機能利用を加えた高度利用の有用な無線電話システムを提供することができる。

【図面の簡単な説明】

【図１】本発明のシステムを実行する配置を示す図である。

【図２】本発明のシステムに使用するプロトコル例のフローを示す流れ図である。

【図３】本発明のシステムに使用するプロトコル例のフローを示す流れ図である。

【図４】本発明のシステムに使用するプロトコル例のフローを示す流れ図である。

【図５】保証制御利用のためのフローを示す流れ図である。

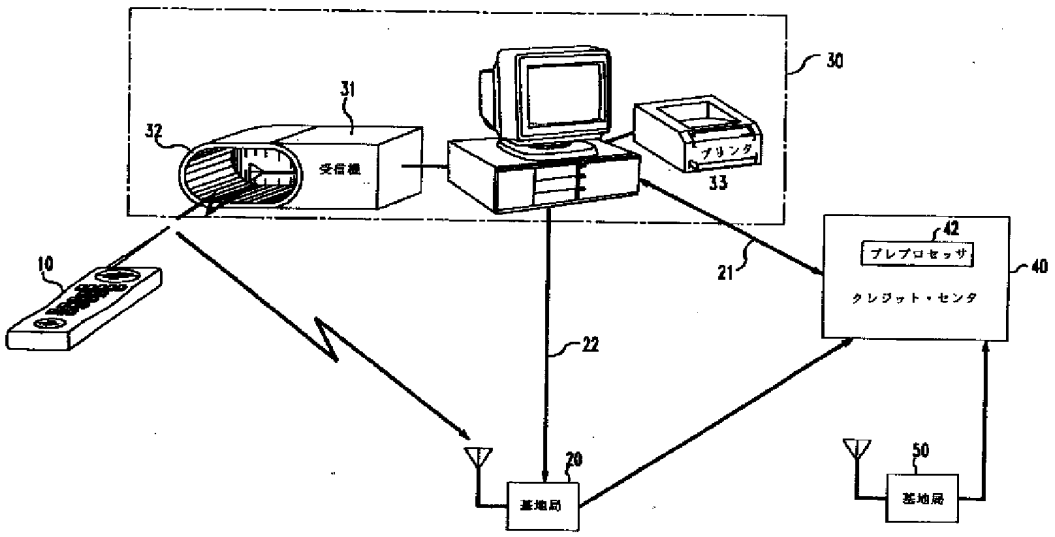
【図６】保証制御利用のためのフローを示す流れ図である。

【図７】ホーム・コントローラ基地局配置を示す図である。

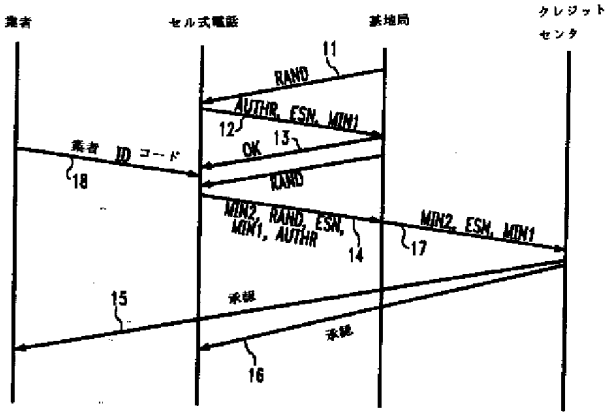
【符号の説明】

１０　セルラ電話
２０　無線電話基地局
２１　チャネル
２２　パス
３０　（販売業者）機器
３１　受信装置
３２　シュラウド
３３　プリンタ
４０　クレジット・センタ
４２　プレプロセッサ
５０　無線電話基地局
６０　ホーム・コントローラ基地局
６１　ホーム・コントローラ
６２　セット・トップ・ボックス
６３　テレビジョン
６４　コントローラ

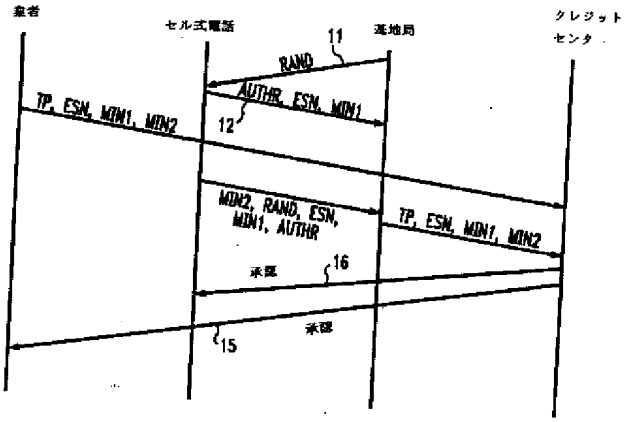
【図１】


30
31
32
受信機
プリンタ
33
10
21
42
プレプロセッサ
クレジット・センタ
40
22
20
基地局
50
基地局

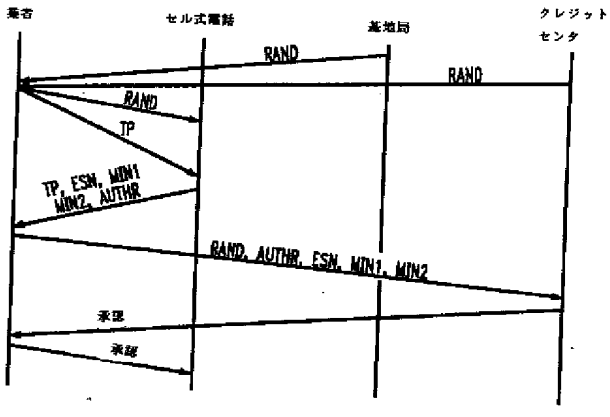
【図２】


基地局
クレジット
センタ
RAND
11
AUTHR, ESN, MIN1
12
OK
13
RAND
MIN2, RAND, ESN,
MIN1, AUTHR
14
MIN2, ESN, MIN1
17
15
承認
承認
16

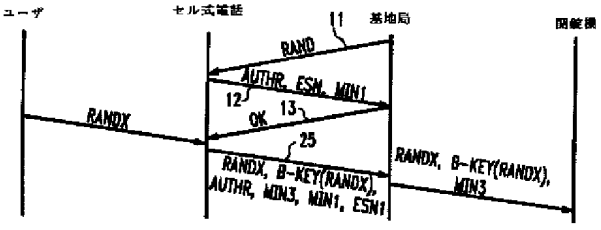
【図３】


セル式電話
基地局
クレジット
センタ
11
RAND
AUTHR, ESN, MIN1
12
TP, ESN, MIN1, MIN2
MIN2, RAND, ESN,
MIN1, AUTHR
TP, ESN, MIN1, MIN2
承認
16
15
承認

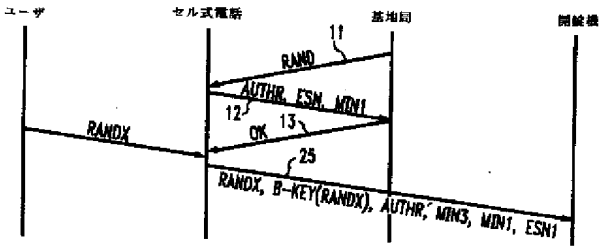
【図４】


セル式電話
基地局
クレジット
センタ
RAND
RAND
RAND
TP
TP, ESN, MIN1
MIN2, AUTHR
RAND, AUTHR, ESN, MIN1, MIN2
承認
承認

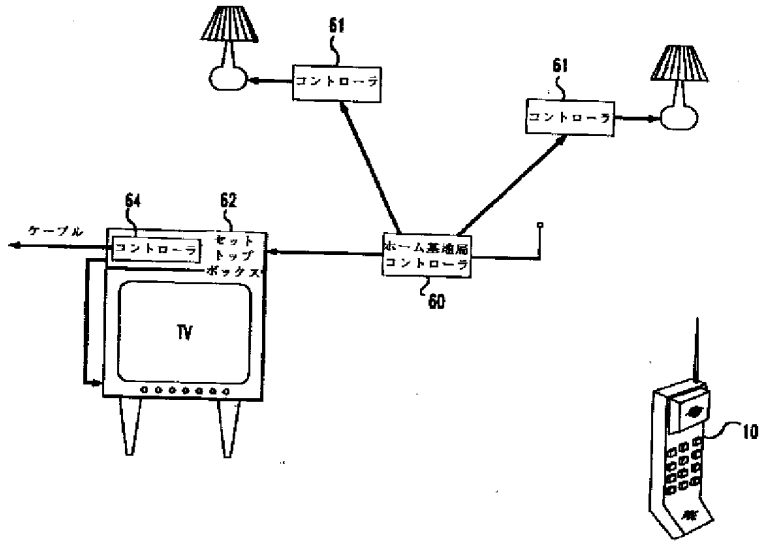
【図５】


ユーザ
セル式電話
11
基地局
RAND
AUTHR, ESN, MIN1
12
13
OK
RANDX
25
RANDX, B-KEY(RANDX),
AUTHR, MIN3, MIN1, ESN1
RANDX, B-KEY(RANDX),
MIN3

【図６】



【図７】



フロントページの続き

(51)Int.Cl.[6]	識別記号	庁内整理番号	ＦＩ		技術表示箇所
			Ｈ０４Ｂ　7/26	１０９　Ｓ	
				１０９　Ｊ	